IT 2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年 ７月３１日

出 願 番 号
Application Number: 平成１０年特許願第２１７７３２号

出 願 人
Applicant (s): 株式会社日立製作所
株式会社日立アドバンストシステムズ
日立京葉エンジニアリング株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年 ３月２６日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

【書類名】　特許願

【整理番号】　HL11836000

【提出日】　平成10年 7月31日

【あて先】　特許庁長官　殿

【国際特許分類】　H04N 7/20

H04L 9/14

【発明の名称】　暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システム

【請求項の数】　22

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内

【氏名】　扇　裕和

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内

【氏名】　高島　英雄

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内

【氏名】　谷口　英宣

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内

【氏名】　高地　宗寿

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内

【氏名】　速水　洋志

出証特平１１－３０１８８９１

【発明者】
【住所又は居所】 神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立アドバンストシステムズ内
【氏名】 浅田　一
【発明者】
【住所又は居所】 千葉県習志野市東習志野７丁目１番１号　日立京葉エンジニアリング株式会社内
【氏名】 原▲崎▼　秀樹
【特許出願人】
【識別番号】 000005108
【氏名又は名称】 株式会社　日立製作所
【特許出願人】
【識別番号】 000153421
【氏名又は名称】 株式会社　日立アドバンストシステムズ
【特許出願人】
【識別番号】 000233217
【氏名又は名称】 日立京葉エンジニアリング株式会社
【代理人】
【識別番号】 100087170
【弁理士】
【氏名又は名称】 富田　和子
【電話番号】 045(316)3711
【手数料の表示】
【予納台帳番号】 012014
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書　1
【物件名】 図面　1
【物件名】 要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システム

【特許請求の範囲】

【請求項１】

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側において、送信側で運用される暗号アルゴリズムを、受信側で運用される暗号アルゴリズムで暗号化して受信側に伝送すること

を特徴とする暗号化通信方法。

【請求項２】

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側で運用される暗号アルゴリズムを、受信側で運用される暗号アルゴリズムで暗号化して送信側に与え、これを受信側に伝送させること

を特徴とする暗号化通信方法。

【請求項３】　請求項２に記載の暗号化通信方法において、

予め送信側に割り当てられた公開鍵に基づいて作成した署名データを、前記暗号化した暗号アルゴリズムと併せて受信側に与えること

を特徴とする暗号化通信方法。

【請求項４】　請求項２及び３のいずれか一項に記載の暗号化通信方法において、

予め送信側に割り当てられた公開鍵に基づいて作成した署名データを、前記暗号化した暗号アルゴリズムと併せて送信側に与え、これを受信側に伝送させること

を特徴とする暗号化通信方法。

【請求項５】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

出証特平１１－３０１８８９１

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項６】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項７】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有

管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項８】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと

、前記送信送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを前記送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項９】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システム。

【請求項１０】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴ暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システム。

【請求項１１】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有

管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項１２】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項１３】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該発信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該発信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項１４】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応し

て前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、前記送信送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項１５】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システム。

【請求項１６】

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴ暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システム。

【請求項１７】

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを、送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること

を特徴とする暗号化通信方法。

【請求項１８】

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること

を特徴とする暗号化通信方法。

【請求項１９】　請求項１８に記載の暗号化通信方法において、

予め受信側に割り当てられた公開鍵に基づいて作成した署名データを、前記暗号化した暗号アルゴリズムと併せて送信側に与えること

を特徴とする暗号化通信方法。

【請求項２０】

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

送信側のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子および当該ユーザが運用可能な暗号アルゴリズムの関係が各ユーザについて予め記述されたデータベースを検索して、前記送信側のユーザが運用可能な暗号アルゴリズム、並びに、受信側のユーザが運用可能な暗号アルゴリズムを取得し、

送信側ユーザおよび受信側ユーザに共通して運用可能な暗号アルゴリズムが存在するか否かを判定し、

前記共通して運用可能な暗号アルゴリズムが存在するとき、前記送信側ユーザおよび受信側ユーザにおける暗号化通信が可能であることを前記送信側ユーザに通知すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項２１】

請求項２０記載の暗号アルゴリズム共有管理方法において、

前記共通して運用可能な暗号アルゴリズムが存在するとき、当該暗号アルゴリズムを示す情報を前記送信側ユーザに送信し、

前記共通して運用可能な暗号アルゴリズムが存在するとき、前記送信側ユーザおよび受信側ユーザにおける暗号化通信が不可能であることを前記送信側ユーザに通知すること

を特徴とする暗号アルゴリズム共有管理方法。

【請求項２２】

運用されている第１の暗号アルゴリズムを、それと別の第２の暗号アルゴリズムに変換するための暗号アルゴリズム変換方法において、

暗号アルゴリズムを変換すべき対象のユーザをキーとして、ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記対象のユーザで運用されている第１の暗号アルゴリズム及び第１の暗号鍵を取得し、

予め管理用に割り当てられた、前記第１の暗号アルゴリズム上で運用される第１の管理用秘密鍵で、前記第１および第２の暗号鍵にそれぞれ署名した第１および第２の署名データと、予め管理用に割り当てられた前記第の２暗号アルゴリズム上で運用される第２の管理用秘密鍵に対応する第２の公開鍵を、前記第１の暗号アルゴリズムで暗号化した公開鍵データと、前記第１の暗号アルゴリズムで暗号化した第２の暗号アルゴリズムと、前記第２の管理用秘密鍵に基づいて作成した署名データとを、前記対象のユーザに与えること

を特徴とする暗号アルゴリズム変換方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

暗号化通信における暗号アルゴリズムを他の暗号アルゴリズムに変換するための、暗号化通信方法、暗号アルゴリズム共有管理方法、ネットワーク通信システ

ムに係り、特に、複数のユーザで運用される暗号アルゴリズムが同一の暗号アルゴリズムを共有したり、共有する暗号アルゴリズムを他の暗号アルゴリズムに変更することに好適な、暗号化通信方法、暗号アルゴリズム共有管理方法、ネットワーク通信システムに関する。

【０００２】

【従来の技術】

情報伝達の安全性を確保する手段としては、伝達する情報を暗号化して通信する方法が一般的である。近年、パーソナルコンピュータの性能の向上により、伝達する情報が文書、映像などのデジタル情報の場合、ソフトウェアで暗号化する方法が採用されることも多い。

【０００３】

ユーザU〔A〕とユーザU〔B〕とが暗号化通信を行う場合、ユーザU〔A〕は、伝達する情報を暗号化用の鍵で暗号化してデータを送信する。一方、これを受信したユーザU〔B〕は、受信したデータを復号化用の鍵で復号化する。このような暗号化通信は、ユーザU〔A〕とユーザU〔B〕とが同一の暗号アルゴリズムを共有していることを前提として成り立つ。通常、暗号システムの管理者が暗号アルゴリズムをフロッピーディスクなどの記憶媒体に記録して各ユーザに配布するか、暗号アルゴリズムが実行可能にインストールされた暗号処理機能を有する情報処理装置を配布するなどの方法でアルゴリズムを共有するようにしている。

【０００４】

また、暗号アルゴリズムを運用する方法としては、暗号のセキュリティを向上させるため、情報を暗号化するための鍵として、スクランブル鍵を生成するばかりでなく、これとは別にこのスクランブル鍵を暗号化するためのセッション鍵を生成し、ユーザU〔A〕は、ユーザU〔B〕にスクランブル鍵で暗号化した情報と、セッション鍵で暗号化したスクランブル鍵を送付する二重暗号化方式がとられ、暗号化通信が発生するごとに、スクランブル鍵を変更するようにしている。

【０００５】

【発明が解決しようとする課題】

（１）送信側及び受信側で、運用するアルゴリズムが相異なる場合には、暗号化通信を行うことはできない。従って、送信側及び受信側の少なくともいずれかに暗号アルゴリズムを配布する必要が生じる。

【０００６】

ところが、上述した、記憶媒体に記録して各ユーザに配布する方法、暗号アルゴリズムが実行可能にインストールされた暗号機能を有する情報処理装置を配布する方法では、輸送、運送などの手段にたよるため、配布そのものに時間を要する。

【０００７】

また、各ユーザに暗号アルゴリズムが配布されると、暗号アルゴリズムをインストールした暗号処理装置と通信機能を有する装置と接続してシステムを構築し、暗号化通信が実施できるか否かの機能確認を行う。この機能確認も、各ユーザ相互に連絡をとりながら実施するため、時間と手間を要する。

【０００８】

（２）また、暗号のセキュリティを向上させる方法として、本発明者らの検討によれば、暗号アルゴリズムを定期的に変更して運用することが考えられる。例えば、上述した二重暗号方式におけるセッション鍵の暗号アルゴリズムを定期的に変更するとさらに、セキュリティの向上が期待される。ところが、このためには変更される暗号アルゴリズムを各ユーザに配信する必要がある。この暗号アルゴリズムの配信を前記（１）と同様の配布方法をとったのでは、時間と手間を要し効率が悪くなる。

【０００９】

（３）近年、パーソナルコンピュータなどの情報機器の進歩に伴ない、情報処理速度は年々向上している。暗号アルゴリズムの強度は、このような情報機器をもちいて解読しようと攻撃してきた場合であっても、情報の有効な期限範囲において解読されないような強度である必要がある。

【００１０】

ところが、運用する暗号アルゴリズムを常に同一とした場合、情報処理速度の向上により、いつかは解読される危険にさらされることになる。

【００１１】

このため、暗号アルゴリズムの強度は、使用される時代の情報機器の情報処理速度に合わせて設定し、強度を高めた暗号アルゴリズムへ変更する必要があり、（２）と同様効率の良い暗号アルゴリズムの配布方法が必要となる。

【００１２】

（４）複数のユーザと、暗号アルゴリズムを運用する鍵を管理する局とが接続される構成として暗号化通信システムを構築することが、本発明者らにより検討されている。ところが、暗号化通信システムに複数の暗号アルゴリズムが混在し、それらの暗号アルゴリズムを定期的に更新するようにすると、このようなシステムには、各ユーザの暗号アルゴリズムを把握し、通信しようとするユーザ相互のアルゴリズムが異なる場合は、同一のアルゴリズムを共有できるようアルゴリズムを配信し、ユーザがアルゴリズムを変更中は、変更中のユーザに関する暗号化通信を停止させるなど、複雑なシステムの運用機能が必要となる。しかし、（１）の暗号アルゴリズムの配布方法をとるとすると、時間と手間を要するばかりでなく、各ユーザの暗号アルゴリズムの状態をリアルタイムに把握するのが難しく、暗号化通信システムが混乱し効率的なシステムの運用が妨げられるおそれがある。

【００１３】

（５）暗号アルゴリズムを変更する場合、ユーザが使用する鍵は、変更する暗号アルゴリズムに対応できない可能性がある。

【００１４】

共通鍵暗号アルゴリズムから公開鍵暗号アルゴリズムへ変更する場合、または、その逆に公開鍵暗号アルゴリズムから共通鍵暗号アルゴリズムに変更する場合は、ユーザが使用する鍵は変更した暗号アルゴリズムには使用できないという問題を生じる。

【００１５】

また、暗号アルゴリズムを強度の高い暗号アルゴリズムに変更した場合、通常は使用する鍵長は長くなる。このため、ユーザが使用する鍵をそのまま変更した暗号アルゴリズムで使用できたとしても、同じ鍵長では、使用しているユーザに対して、暗号強度が増さないという問題を生じる。

【００１６】

本発明は、上述のような状況に鑑みてなされたものであり、暗号アルゴリズムの配信を安全に、しかも、それに要する時間と手間を削減した状態で、暗号アルゴリズムを変換することができる、暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システムを提供することを目的とする。

【００１７】

また、このような暗号アルゴリズムの変換によって、複数のユーザで運用される暗号アルゴリズムが同一の暗号アルゴリズムを共有したり、共有する暗号アルゴリズムを他の暗号アルゴリズムに変更することに好適な、暗号化通信方法、暗号アルゴリズム共有管理方法、暗号アルゴリズム変換方法、ネットワーク通信システムを提供することをも目的とする。

【００１８】

【課題を解決するための手段】

前記目的を達成するために、本発明の第１の態様によれば、

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側において、送信側で運用される暗号アルゴリズムを、受信側で運用される暗号アルゴリズムで暗号化して受信側に伝送すること

を特徴とする暗号化通信方法が提供される。

【００１９】

本発明の第２の態様によれば、

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、送信側で運用される暗号アルゴリズムを、

受信側で運用される暗号アルゴリズムで暗号化して送信側に与え、これを受信側に伝送させること

を特徴とする暗号化通信方法が提供される。

【００２０】

本発明の第３の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２１】

本発明の第４の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運

用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２２】

本発明の第５の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２３】

本発明の第６の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、前記送信送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを前記送信先相手のユーザに送信させること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２４】

本発明の第７の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システムが提供される。

【００２５】

本発明の第８の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応

関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴ暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して受信側ユーザに伝送させること

を特徴とするネットワーク通信システムが提供される。

【００２６】

本発明の第９の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムを検索し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムを表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２７】

本発明の第１０の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵を表すデータを、前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化して当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２８】

本発明の第１１の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズム及び送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、当該発信元のユーザが運用する暗号鍵に対して作成した署名データを前記発信元ユーザに送信するとともに、当該発信元のユーザが運用する暗号アルゴリズムを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、当該発信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該発信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００２９】

本発明の第１２の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

発信元のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が、各ユーザについて予め記述されたデータベースを検索して、前記発信元のユーザが運用する暗号アルゴリズム及び暗号鍵、並びに、送信先相手のユーザが運用する暗号アルゴリズム及び暗号鍵を取得し、

前記発信元のユーザが運用する暗号アルゴリズムおよび送信先相手のユーザが運用する暗号アルゴリズムが相違するとき、前記発信元のユーザが運用する暗号鍵に対して作成した署名データを発信元ユーザに送信するとともに、前記発信元のユーザが運用する暗号アルゴリズムと、当該暗号アルゴリズムの鍵長に対応して前記送信先相手のユーザが運用する暗号鍵を基に作成した暗号鍵とを表すデータを前記送信先相手のユーザが運用する暗号アルゴリズムで暗号化したデータと、前記送信送信先相手のユーザが運用する暗号鍵に対して作成した署名データとを当該送信先相手のユーザに送信すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００３０】

本発明の第１３の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、送信側ユーザから、当該ユーザで運用される暗号アルゴリズムを示す情報と、受信側ユーザで運用される暗号アルゴリズムを示す情報とを取得し、送信側ユーザ及び受信側ユーザで相異なる暗号アルゴリズムが運用されるとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システムが提供される。

【００３１】

本発明の第１４の態様によれば、

複数のユーザが接続されて構成されるネットワーク通信システムにおいて、

少なくとも送信側となるユーザから接続される暗号鍵管理局を備え、

前記暗号鍵管理局は、

ユーザを示すユーザ識別子及び当該ユーザが運用する暗号アルゴリズムの対応関係が、各ユーザについて予め記述されたデータベースを有し、

送信側ユーザから受信側ユーザに通信が行われるに際し、送信側ユーザから、当該ユーザを示すユーザ識別子と、受信側ユーザ識別子とを取得し、前記取得した識別子をキーとして前記データベースを検索して、前記送信側ユーザが運用する暗号アルゴリズムと、受信側のユーザが運用する暗号アルゴ暗号アルゴリズムとを求め、

送信側ユーザと受信側ユーザとで、運用される暗号アルゴリズムが相違するとき、送信側ユーザで運用される暗号アルゴリズムを、受信側ユーザで運用される暗号アルゴリズムで暗号化して当該受信側ユーザに伝送すること

を特徴とするネットワーク通信システムが提供される。

【００３２】

本発明の第１５の態様によれば、

送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを、送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること

を特徴とする暗号化通信方法が提供される。

【００３３】

本発明の第１６の態様によれば、

送信側から、送信側で運用される暗号アルゴリズムを示す情報と、受信側で運用される暗号アルゴリズムを示す情報とを取得し、送信側及び受信側で相異なる暗号アルゴリズムが運用されるとき、受信側で運用される暗号アルゴリズムを送信側で運用される暗号アルゴリズムで暗号化して当該送信側に伝送すること

を特徴とする暗号化通信方法が提供される。

【００３４】

本発明の第１７の態様によれば、

暗号化通信における暗号アルゴリズムを共有するための暗号アルゴリズム共有管理方法であって、

送信側のユーザから、当該ユーザを示すユーザ識別子及び送信先相手のユーザを示すユーザ識別子を取得し、

ユーザを示すユーザ識別子および当該ユーザが運用可能な暗号アルゴリズムの関係が各ユーザについて予め記述されたデータベースを検索して、前記送信側のユーザが運用可能な暗号アルゴリズム、並びに、受信側のユーザが運用可能な暗号アルゴリズムを取得し、

送信側ユーザおよび受信側ユーザに共通して運用可能な暗号アルゴリズムが存在するか否かを判定し、

前記共通して運用可能な暗号アルゴリズムが存在するとき、前記送信側ユーザおよび受信側ユーザにおける暗号化通信が可能であることを前記送信側ユーザに通知すること

を特徴とする暗号アルゴリズム共有管理方法が提供される。

【００３５】

本発明の第１８の態様によれば、

運用されている第１の暗号アルゴリズムを、それと別の第２の暗号アルゴリズムに変換するための暗号アルゴリズム変換方法において、

暗号アルゴリズムを変換すべき対象のユーザをキーとして、ユーザを示すユーザ識別子並びに当該ユーザが運用する暗号アルゴリズム及び暗号鍵の対応関係が各ユーザについて予め記述されたデータベースを検索して、前記対象のユーザで運用されている第１の暗号アルゴリズム及び第１の暗号鍵を取得し、

予め管理用に割り当てられた、前記第１の暗号アルゴリズム上で運用される第１の管理用秘密鍵で、前記第１および第２の暗号鍵にそれぞれ署名した第１および第２の署名データと、予め管理用に割り当てられた前記第の２暗号アルゴリズム上で運用される第２の管理用秘密鍵に対応する第２の公開鍵を、前記第１の暗

号アルゴリズムで暗号化した公開鍵データと、前記第１の暗号アルゴリズムで暗号化した第２の暗号アルゴリズムと、前記第２の管理用秘密鍵に基づいて作成した署名データとを、前記対象のユーザに与えること

を特徴とする暗号アルゴリズム変換方法が提供される。

【００３６】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態について説明する。

【００３７】

まず、本発明を適用したネットワーク通信システムの概略の作用について説明する。

【００３８】

本発明を適用した暗号通信システムでは、（１）暗号アルゴリズムを管理する鍵管理局を設置し、当該鍵管理局によって、（２）各ユーザが運用する暗号アルゴリズムの状態を掌握し、（３）各ユーザが使用する暗号アルゴリズムを設定し、（４）各ユーザの使用する暗号アルゴリズムを変換する。以下に、それぞれにおける作用について説明する。

【００３９】

（１）まず、暗号アルゴリズムを管理する鍵管理局について説明する。

【００４０】

暗号化通信システムに、暗号アルゴリズムを管理する鍵管理局を設置し、各ユーザが使用する暗号アルゴリズム及び更新する暗号アルゴリズムはすべてこの鍵管理局に登録するものとする。

【００４１】

（２）次に、各ユーザの運用する暗号アルゴリズムの状態を掌握する作用について説明する。

【００４２】

暗号化通信を行う各ユーザと鍵管理局とは、衛星通信回線または地上回線等の電子通信回線で接続し、鍵管理局は常にこの回線を通して各ユーザの運用する暗号アルゴリズムの状態を掌握し、各ユーザ間で暗号化通信の必要が生じた場合、

当該ユーザが運用する暗号アルゴリズムの運用状態から暗号化通信が可能か判断するものとする。

【００４３】

また、鍵管理局は、各ユーザの暗号アルゴリズムの運用状態とともに、当該ユーザの使用する鍵の情報についても掌握しており、当該ユーザの運用する暗号アルゴリズムを変更した場合、当該ユーザの使用する鍵を変更した暗号アルゴリズムに適応できるよう、鍵を変換する情報を作成し、当該ユーザに伝達するものとする。

【００４４】

（３）次に、各ユーザが使用する暗号アルゴリズムを設定する作用について、（ｉ）各ユーザ相互に暗号化通信を実施する場合と、（ｉｉ）各ユーザが使用する暗号アルゴリズムの強度を、同等以上の同一系列の暗号アルゴリズムに変換する場合とのそれぞれについて順次説明する。

【００４５】

まず、（ｉ）各ユーザ相互に暗号化通信を実施する場合について説明する。

【００４６】

取り得る場合としては、（ａ）暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有している場合と、（ｂ）暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有していない場合とがある。以下にそれぞれの場合に対応した作用について説明する。

【００４７】

（ａ）暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有している場合

１：鍵管理局は、当該ユーザ相互の暗号化通信が可能と判断し、当該ユーザ相互にこの判断結果を伝達する。

【００４８】

２：当該ユーザは、この結果を受けて共有している暗号アルゴリズムにより暗号化通信を実施する。

【００４９】

（ｂ）暗号化通信を実施するユーザ相互が同一の暗号アルゴリズムを共有していない場合

１：鍵管理局は、当該ユーザ相互の暗号化通信が不可能と判断する。

【００５０】

２：鍵管理局は、登録されている暗号アルゴリズムの中からユーザの要求、制約等を考慮し、当該ユーザ相互の暗号化通信に使用する暗号アルゴリズムを設定し、この暗号アルゴリズムを当該ユーザに通信回線を通じて伝達する。

【００５１】

また、当該ユーザの使用する鍵を新しく設定した暗号アルゴリズムに適用できるよう変換する必要がある場合は、この鍵変換のための情報を作成し、当該ユーザに通信回線を通じて伝達する。

【００５２】

３：　当該ユーザは、送付された暗号アルゴリズム及び、必要に応じて使用する鍵を変換し、暗号化通信を実施する。

【００５３】

次に、（ｉｉ）各ユーザが使用する暗号アルゴリズムの強度を、同等以上の強度の同一系列の暗号アルゴリズムに変換する場合について説明する。暗号アルゴリズムの強度を、同等以上の強度の同一系列の暗号アルゴリズムに変換するためには、例えば、（ａ）ユーザが使用している暗号アルゴリズムに対して、当該ユーザが同等以上の強度の同一系列の暗号アルゴリズムを提供すること、（ｂ）ユーザが使用しているある暗号アルゴリズムに対して、鍵管理局が暗号アルゴリズム生成装置を所有しており、当該鍵管理局が同等以上の強度の同一系列の暗号アルゴリズムを提供することができる。それぞれの作用について以下に説明する。

【００５４】

（ａ）ユーザが使用している暗号アルゴリズムに対して、当該ユーザが同等以上の強度の同一系列の暗号アルゴリズムを提供する場合

１：ユーザが同等以上の強度の同一系列の暗号アルゴリズムを製作し、当該暗号アルゴリズムを鍵管理局に伝達し、登録する。

【００５５】

２：鍵管理局は、前記暗号アルゴリズムの強度を上げる前の暗号アルゴリズムを使用しているユーザを設定し、必要に応じて当該ユーザの使用している鍵変換のための情報を作成し、このユーザに同等以上の強度の同一系列の暗号アルゴリズムと鍵変換のための情報とを送付する。

【００５６】

３：当該ユーザは、送付された暗号アルゴリズム及び、必要に応じて使用する鍵を変換し、暗号化通信を実施する。

【００５７】

（ｂ）ユーザが使用しているある暗号アルゴリズムに対して、鍵管理局が暗号アルゴリズム生成装置を所有しており、当該鍵管理局が同等以上の強度の同一系列の暗号アルゴリズムを提供する場合

１：　鍵管理局が同等以上の強度の同一系列の暗号アルゴリズムを作成し、当該暗号アルゴリズムを登録する。

【００５８】

２：　鍵管理局は、前記暗号アルゴリズムを変換する前の暗号アルゴリズムを使用しているユーザを設定し、必要に応じて当該ユーザが使用している鍵を変換するためのための情報を作成し、このユーザに同等以上の強度の同一系列の暗号アルゴリズムと鍵変換のための情報とを送付する。

【００５９】

３：　当該ユーザは、送付された暗号アルゴリズム及び、必要に応じて使用する鍵を変換し、暗号化通信を実施する。

【００６０】

（４）次に、各ユーザが使用する暗号アルゴリズムを変換する作用について説明する。

【００６１】

１：　鍵管理局は、上述した（３）に従って、各ユーザの変換する暗号アルゴリズム、及び必要に応じ各ユーザの使用する鍵の変換情報を作成する。

【００６２】

２：　鍵管理局は、各ユーザの変換する暗号アルゴリズム、及び必要に応じて作成した鍵の変換情報を、各ユーザの運用する変換前の暗号アルゴリズムで暗号化し、各ユーザに通信回線を通じて伝達する。

【００６３】

３：　各ユーザは運用している暗号アルゴリズムを使用して、鍵管理局から送付されたデータを復号し変換する暗号アルゴリズム及び鍵の変換情報を取得する。

【００６４】

４：　各ユーザは、前記復号したデータをもとに、運用する暗号アルゴリズムと使用する鍵を変更する。

【００６５】

５：　各ユーザは変更した暗号アルゴリズムをもちいて、「暗号アルゴリズム変更終了」という文を暗号化し通信回線を介して、鍵管理局に送信する。

【００６６】

６：　鍵管理局は、暗号化されて伝達されたデータを復号し、「暗号アルゴリズム変更終了」という文を取得することにより、ユーザの暗号アルゴリズムが変換し、暗号化機能が正常に機能していることを確認する。

【００６７】

次に、図１から図５を参照して、本発明の第１の実施の形態について説明する。本実施の形態では、本発明を適用した暗号アルゴリズム変換の概要について説明する。

【００６８】

まず、図１を参照して、本発明の適用対象となるネットワーク通信システムについて説明する。ここでは、ユーザが使用する複数のパーソナルコンピュータ（情報処理装置）１００，２００と鍵管理局４００とが接続された構成例について説明する。

【００６９】

本システムに運用される暗号アルゴリズムを、Ａ〔１〕～Ａ〔ｎ〕，Ｂ〔１〕

～Ｂ〔ｍ〕とし、これらの暗号アルゴリズムを鍵管理局が管理している。暗号アルゴリズムのＡ〔１〕～Ａ〔ｎ〕は、同一のＡ系列の暗号強度が同一または異なる暗号アルゴリズムであり、暗号強度が同等以上の同一系列の暗号アルゴリズムに変更することによるセキュリテイの更新を鍵管理局が実施している。

【００７０】

暗号アルゴリズムＡ〔１〕を運用するユーザのユーザＩＤをＵ〔A_1，１〕～Ｕ〔A_1，N_1〕、暗号アルゴリズムＡ〔２〕を運用するユーザのユーザＩＤをＵ〔A_2，１〕～Ｕ〔A_2，N_2〕、…、暗号アルゴリズムＡ〔ｎ〕を運用するユーザのユーザＩＤをＵ〔A_n，１〕～Ｕ〔A_n，N_n〕とし、暗号アルゴリズムＢ〔１〕を運用するユーザのユーザＩＤをＵ〔B_1，１〕～Ｕ〔B_1，M_1〕、暗号アルゴリズムＢ〔２〕を運用するユーザのユーザＩＤをＵ〔B_2，１〕～Ｕ〔B_2，M_2〕、…、暗号アルゴリズムＢ〔ｍ〕を運用するユーザのユーザＩＤをＵ〔B_n，１〕～Ｕ〔B_n，M_m〕とし、鍵管理局は各ユーザの運用する暗号アルゴリズムとユーザＩＤを対応させて管理している。

【００７１】

図１において、Ａ系列に属する暗号アルゴリズムのうちの１つ（以下、単に暗号アルゴリズムＡという）を運用するユーザが使用するパーソナルコンピュータ１００と、Ｂ系列に属する暗号アルゴリズムのうちの１つ（以下、単に暗号アルゴリズムＢという）を運用するユーザが使用するパーソナルコンピュータ２００と、鍵管理用ワークステーション５００を備える鍵管理局４００とがネットワークに接続されている。

【００７２】

このネットワーク通信システムでは、暗号化通信、暗号アルゴリズム変換等は、各ユーザが使用する情報処理装置などのパーソナルコンピュータ１００，２００及び、鍵管理用ワークステーション５００のソフト処理によって実施される。

【００７３】

図２２は、複数の暗号アルゴリズムが存在するネットワーク通信システムの図１とは別の形態を示している。この形態のネットワーク通信システムでは、ネットワーク通信システムに、暗号アルゴリズムとして、アルゴリズムＡ、アルゴリ

ズムＢ、アルゴリズムＣ、アルゴリズムＤと、４つの暗号アルゴリズムが混在している。

【００７４】

通常、使用する暗号アルゴリズムは、ユーザが選択して定める。

【００７５】

暗号アルゴリズムの性質から、ユーザが使用したくないものも存在する。

【００７６】

図２２に示されるネットワーク通信システムでは、前記４つの暗号アルゴリズム、Ａ，Ｂ，ＣおよびＤが使用されている。なお、本図において、暗号アルゴリズムＡを使用するユーザの範囲を実線で示し、暗号アルゴリズムＢを使用するユーザの範囲を一点鎖線で示し、暗号アルゴリズムＡを使用するユーザの範囲を二点鎖線で示し、暗号アルゴリズムＤを使用するユーザの範囲を破線で示している。

【００７７】

各暗号アルゴリズムの使用範囲が、重なっている部分のユーザは、複数の暗号アルゴリズムを使用することができる。

【００７８】

鍵管理局は、各暗号アルゴリズムに対して、その暗号アルゴリズムを使用可能なユーザをデータベースに格納している。

【００７９】

各ユーザ間で、暗号化通信要求が発生した場合、鍵管理用ワークステーションは、前記データベースに基づき、送信側及び受信側それぞれの暗号アルゴリズムの運用状態を把握する。

【００８０】

送信側及び受信側で同一の暗号アルゴリズムを共有している場合は、両者の暗号化通信を続行させる。

【００８１】

同一の暗号アルゴリズムを共有していない場合、前記データベースに基づき、送信側及び受信側ユーザに同一の暗号アルゴリズムを持たせることが可能か否か

を判断する。

【００８２】

共有させることができない場合は、両者に暗号化通信ができないことを連絡する。

【００８３】

ユーザ相互に暗号アルゴリズムを共有できるかどうかは、ユーザの都合によって定まるものである。

【００８４】

各暗号アルゴリズムを使用するユーザの範囲は、ユーザの都合によって変化する。

【００８５】

鍵管理用ワークステーションは、ユーザ等の連絡により各暗号アルゴリズムを使用するユーザを示すデータベースに格納される情報を変更するものとする。

【００８６】

次に、図２を参照して、本ネットワーク通信システムにおける各情報処理装置（パーソナルコンピュータ、鍵管理用ワークステーション）が備えるソフト処理機能について説明する。

【００８７】

図２において、パーソナルコンピュータ１００及び２００とが接続されてネットワークが構成されている。以下、パーソナルコンピュータ１００が送信側ユーザに使用され，パーソナルコンピュータ２００が受信側ユーザに使用される場合について説明する。なお、パーソナルコンピュータ１００及び２００は同様に構成されるので、これらは、送信側、受信側のいずれにも使用することが可能であることは勿論である。また、鍵管理用ワークステーション５００が、少なくとも送信側ユーザに使用されるパーソナルコンピュータ１００と接続されている。

【００８８】

前記送信側（受信側）ユーザが使用するパーソナルコンピュータ１００（２００）は、鍵構成管理機能１１０（２１０）と、暗号アルゴリズム管理機能１２０（２２０）と、スクランブル機能１３０（２３０）と、デスクランブル機能１４

０（２４０）と、暗号化通信管理機能１５０（２５０）とを備え、鍵構成管理データベース１８０（２８０）と、暗号アルゴリズムデータベース１９０（２９０）とをアクセス可能に接続されている。

【００８９】

なお、これらのデータベースは、パーソナルコンピュータ１００，２００と別個に備えられてもよいし、パーソナルコンピュータ１００，２００と一体に構成されてもよい。また、前記データベースは、複数のパーソナルコンピュータで共有されていてもよい。

【００９０】

前記鍵管理用ワークステーション５００は、スクランブル機能５３０と、デスクランブル機能５４０と、暗号化通信管理機能５５０と、暗号アルゴリズム生成機能５９５と、ネットワーク暗号管理機能５６０と、ネットワーク鍵管理機能５７０とを備え、ネットワーク暗号アルゴリズム管理データベース５９０と、ネットワーク鍵管理データベースとにアクセス可能に接続される。なお、これらのデータベースは、鍵管理用ワークステーション５００と別個に設置されてもよいし、鍵管理用ワークステーション５００と一体に構成されてもよい。

【００９１】

次に、同じく図２を参照して、鍵管理用ワークステーション５００の機能について説明する。

【００９２】

ネットワーク暗号アルゴリズム管理ＤＢ５９０には、各ユーザのユーザＩＤと暗号アルゴリズムとを対応させて登録している。

【００９３】

ネットワーク暗号アルゴリズム管理機能５７０は、前記２組のデータに関するＤＢを管理しており、各ユーザの使用する暗号アルゴリズムの、登録、更新、削除を実施している。

【００９４】

暗号アルゴリズム生成機能５９５は、Ａ系列の暗号アルゴリズムを生成する機能を有している。

【００９５】

暗号アルゴリズムの暗号強度は、運用する鍵の鍵長が長くなると暗号解読がより困難になり暗号強度が増加してセキュリテイを改善することができる。

【００９６】

また、同じ鍵長の暗号アルゴリズムでも定期的に運用する暗号アルゴリズムを変更すれば、暗号アタックの期間を限定することができ、通信上のセキュリティを改善することができる。

【００９７】

暗号アルゴリズム生成機能５９５は、使用する鍵長が同じものか、または、鍵長が長くなるような、Ａ系列における相異なる暗号アルゴリズムを生成している。

【００９８】

ネットワーク鍵構成管理機能５７０は、本システムで運用される鍵を管理し、ネットワーク鍵構成管理ＤＢにユーザの使用する鍵情報を格納している。

【００９９】

スクランブル機能５３０は、鍵管理局４００（図１参照）がユーザに送信するデータを暗号化する機能であり、デスクランブル機能５４０は、鍵管理局４００（図１参照）がユーザから受信した暗号化されたデータを復号するための機能である。

【０１００】

ネットワーク鍵管理機能５７０は、暗号化、復号化に使用する鍵の管理を実施しており、鍵構成管理ＤＢ１８０，２８０に運用する暗号アルゴリズムに対応させて各ユーザが使用する鍵に関する情報を格納している。

【０１０１】

次に、前記ユーザが使用する情報処理装置などのパーソナルコンピュータ１００（２００）のソフト機能について説明する。

【０１０２】

暗号アルゴリズム管理機能１２０（２２０）は、ユーザが運用する暗号アルゴリズムを管理している。

【０１０３】

運用する暗号アルゴリズムは、鍵管理用ワークステーション５００の指示により、暗号アルゴリズムを変換する。暗号アルゴリズム管理ＤＢには、鍵管理局４００（図１参照）より配布される暗号アルゴリズムを格納している。

【０１０４】

スクランブル機能１３０（２３０）は、ユーザが送信するデータを暗号化する機能であり、デスクランブル機能１４０（２４０）は、ユーザが受信した暗号化されたデータを復号する機能である。

【０１０５】

鍵構成管理機能１１０（２１０）は、暗号化、復号化に使用する鍵の管理を実施しており、鍵構成管理ＤＢ１８０（２８０）に運用する暗号アルゴリズムに対応させて鍵を格納している。

【０１０６】

次に、図３を参照して、前記鍵管理用ワークステーションからアクセスされるデータベースに格納される情報の内容について説明する。

【０１０７】

図３の（ａ）において、ネットワーク暗号アルゴリズム管理データベースには、ユーザを識別するためのユーザＩＤと、当該ユーザが運用する暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンとの対応関係が記述され、さらのその更新日時が記述された情報、及び、鍵管理局を識別するための鍵管理局ＩＤと、当該鍵管理局が運用する暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンとの対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【０１０８】

図３の（ｂ）において、ネットワーク鍵管理データベースには、ユーザを識別するためのユーザＩＤと、当該ユーザが運用する暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンと、運用される暗号鍵を示す鍵情報との対応関係が記述され、さらのその更新日時が記述された情報、及び、鍵管理局を識別するための鍵管理局ＩＤと、当該鍵管理局が運用する暗号アルゴリズムの

暗号アルゴリズム名及び暗号アルゴリズムバージョンと、運用される暗号鍵を示す鍵情報との対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【０１０９】

次に、図４を参照して、前記ユーザが使用するパーソナルコンピュータからアクセスされるデータベースに格納される情報の内容について説明する。

【０１１０】

図４の（ａ）において、暗号アルゴリズム管理データベースには、暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンの対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【０１１１】

図４の（ｂ）において、鍵管理データベースには、暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンと、ユーザの暗号鍵を示すユーザ鍵情報との対応関係が記述され、さらのその更新日時が記述された情報、及び、暗号アルゴリズムの暗号アルゴリズム名及び暗号アルゴリズムバージョンと、鍵管理局の暗号鍵を示す鍵管理局の鍵情報との対応関係が記述され、さらのその更新日時が記述された情報が格納されている。

【０１１２】

次に、図７を参照して、送信、受信双方のユーザが同一の暗号アルゴリズム（ここでは、共通鍵暗号が運用されているものとする）を共有している場合の暗号化通信の概要について説明する。この場合、送信側ユーザをＡとし、受信側ユーザをＢとし、これらの間で伝送される送信データをＭとする。

【０１１３】

ユーザＵ〔Ａ〕は、鍵管理用ワークステーション５００に対してユーザＵ〔Ｂ〕を指定し、暗号通信に用いるセッション鍵発行要求を行う。

【０１１４】

鍵管理用ワークステーション５００は、この要求を受け、ユーザＵ〔Ｂ〕と暗号通信を可能とするセッション鍵をユーザＵ〔Ｂ〕に発行する。

【０１１５】

ユーザＵ〔Ａ〕は、このセッション鍵の発行を受けると、自分が使用するパーソナルコンピュータのスクランブル機能１３０と組み合わせて、データＭを暗号化し、暗号文としてユーザＵ〔Ｂ〕に送付する。

【０１１６】

ユーザＵ〔Ｂ〕は、ユーザＵ〔Ａ〕と同じ暗号アルゴリズムを暗号アルゴリズムＤＢ１９０に格納している。これより、ユーザＵ〔Ｂ〕は、ユーザＵ〔Ａ〕から送付された、暗号文をデスクランブル機能１４０より復号しデータＭを取得する。

【０１１７】

一方、送信、受信双方のユーザで、運用される暗号アルゴリズムが相違する場合として、例えば、運用する暗号アルゴリズムＡ〔１〕～Ａ〔ｎ〕，Ｂ〔１〕～Ｂ〔ｍ〕が、共通鍵暗号アルゴリズム、公開鍵暗号アルゴリズムの方式が相異なる複数の暗号アルゴリズムが混在していることがある。

【０１１８】

ユーザＵ〔Ａ〕がユーザＵ〔Ｂ〕に暗号化通信を実施する場合、双方のユーザが同一の暗号アルゴリズムを共有している場合は、そのまま暗号化通信を実施できるが、同一の暗号アルゴリズムを共有していない場合は、ユーザが所有する暗号アルゴリズムを変換し双方のユーザに同一の暗号アルゴリズムを共有させて、暗号化通信を実施する。

【０１１９】

この暗号アルゴリズムの変換は、ユーザの所有する暗号アルゴリズムの状態に応じて、下記に示すような暗号アルゴリズム変換を実施する。

【０１２０】

（１）同一系列の暗号アルゴリズムは、バージョン番号で管理し、同じ暗号強度を有する他の暗号アルゴリズム、または、異なる暗号強度を有する他の暗号強度を暗号アルゴリズムへ変換する。

【０１２１】

（２）共通鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへ変換する。

【０１２２】

（３）公開鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへ変換する。

【０１２３】

（４）共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへ変換する。

【０１２４】

（５）公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへ変換する。

【０１２５】

ここで言う、暗号アルゴリズムとは、一連のデータの変換手順を指すものである。

【０１２６】

暗号化とは、データの変換を意味し、復号とは変換されたデータの逆変換を意味している。

【０１２７】

例えば、Ｋを二進法のデータ列とし、Ｍを別の二進法のデータ列とする。

【０１２８】

このＫが定める以下のπ関数を考える。

【０１２９】

$\pi(M) = M \ \mathrm{xor} \ K$

ここで、ｘｏｒは、ＭとＫとの排他的論理和を示している。

【０１３０】

π（Ｍ）により、データＭは、変換された。この変換されたデータに対して、

$\pi(M) \ \mathrm{xor} \ K$

を求めると、

$$\pi(M) \ \mathrm{xor} \ K = (M \ \mathrm{xor} \ K) \ \mathrm{xor} \ K$$
$$= M \ \mathrm{xor} \ (K \ \mathrm{xor} \ K)$$
$$= M$$

となり、変換されたデータπ（Ｍ）からデータＭが逆変換された。

【０１３１】

このπ関数のような、データの変換及び逆変換の手順を暗号アルゴリズムと呼

ぶ。

【０１３２】

次に、Ｎ個のデータの組｛K_1，K_2，K_3，…，K_N｝を考え、ｉ番目のデータK_iに対応する関数をπ_iとする。このＮ個のπ関数から次の２組の関数ｆ，ｇを考える。

【０１３３】

$f = \pi_1 \circ \pi_2 \circ \pi_3 \circ \circ \circ \pi_N$

$g = \pi_N \circ \pi_{N-1} \circ \pi_{N-2} \circ \circ \circ \pi_1$

この２組の関数ｆ，ｇは、このｎ個のπ関数の演算をＮ回繰り返したものである。

【０１３４】

従って、ｆ（Ｍ）、ｇ（Ｍ）は、それぞれデータＭの変換手順を示し、変換されたデータｆ（Ｍ）は、関数ｇによって逆変換され、データＭが導出される。

【０１３５】

このため、関数ｆ，ｇは、１つの暗号アルゴリズムと考えることができ、関数ｆは、データの暗号化に対応し、関数ｇは、データの復号化に対応するものと考えられる。

【０１３６】

Ｎ個のπ関数の演算順序や、パラメータK_iの値を変更すると、別の暗号アルゴリズムが得られる。

【０１３７】

前述の暗号アルゴリズム変換で述べた同一系列の暗号アルゴリズムとは、このようにデータ変換の一部の順序を変更したり、使用するパラメータの値を変えて組み立てた暗号アルゴリズムを指すものである。同一系列の暗号アルゴリズムのことを、以降、バージョンが異なる暗号アルゴリズムと呼ぶことにする。

【０１３８】

このような、暗号アルゴリズム変換を実施する場合、ユーザが所有する鍵も、変換した暗号アルゴリズムにあわせて変換を実施する。

【０１３９】

次に、図５を参照して、本発明を適用した、ネットワーク通信で運用する暗号アルゴリズム変換の概要について説明する。

【０１４０】

ここで、送信側ユーザをＵ〔Ａ〕とし、Ｕ〔Ａ〕が運用している暗号アルゴリズムを暗号アルゴリズムＥＡＮＧとする。一方、受信側ユーザをＵ〔Ｂ〕とし、Ｕ〔Ｂ〕が運用している暗号アルゴリズムを暗号アルゴリズムＥＢＦとする。

【０１４１】

鍵管理用ワークステーション５００のネットワーク暗号アルゴリズム管理ＤＢ５９０には、暗号アルゴリズムＥＡＮＧをユーザＵ〔Ａ〕のユーザＩＤと対応させ、暗号アルゴリズムＥＢＦをユーザＵ〔Ｂ〕のユーザＩＤと対応させて、格納している。

【０１４２】

また、暗号アルゴリズムＥＡＮＧで鍵管理用ワークステーション５００が、ユーザＵ〔Ａ〕と暗号化通信を実施するための鍵をK_Aとし、暗号アルゴリズムＥＢＦで鍵管理用ワークステーション５００が、ユーザＵ〔Ｂ〕と暗号化通信を実施するための鍵をK_Bとする。

【０１４３】

ユーザＵ〔Ａ〕の鍵構成管理ＤＢ（図示せず）には、鍵K_Aが格納されており、ユーザＵ〔Ｂ〕の鍵構成管理ＤＢ１８０には、鍵K_Bが格納されており、鍵管理用ワークステーション５００のネットワーク鍵管理ＤＢ５８０には、ユーザＵ〔Ａ〕のユーザＩＤと対応させて鍵K_Aを格納し、ユーザＵ〔Ｂ〕のユーザＩＤと対応させて鍵K_Bを格納している。

【０１４４】

以上の環境のもとで、ユーザＵ〔Ａ〕がユーザＵ〔Ｂ〕に暗号化通信を実施する場合を例にして、本ネットワーク通信システムで運用する暗号アルゴリズム変換について概略を説明する。

【０１４５】

１：　ユーザＵ〔Ａ〕は、暗号化通信管理機能１５０より、送信相手をユーザ

Ｕ〔Ｂ〕のユーザＩＤで指定し＜セッション鍵発行要求＞を鍵管理ワークステーション５００の暗号化通信管理機能５５０に送付する。

【０１４６】

２：　＜セッション鍵発行要求＞は、鍵管理ワークステーション５００のネットワーク暗号アルゴリズム管理機能５６０に送付される。ネットワーク暗号アルゴリズム管理機能５６０は、ユーザＵ〔Ａ〕のユーザＩＤと、ユーザＵ〔Ｂ〕のユーザＩＤとに基づいて、ネットワーク暗号アルゴリズムＤＢ５９０の検索を行う。

【０１４７】

ユーザＵ〔Ａ〕が運用する暗号アルゴリズムは暗号アルゴリズムＥＡＮＧであり、ユーザＵ〔Ｂ〕の暗号アルゴリズムは暗号アルゴリズムＥＢＦである。このため、同一の暗号アルゴリズムを共有していないと判断し、この結果を暗号化通信管理機能５５０に送付する。

【０１４８】

３：　この結果を受けて、暗号化通信管理機能５５０は、ユーザＵ〔Ｂ〕の暗号アルゴリズムをＥＢＦからＥＡＮＧへの変換動作を始める。

【０１４９】

まず、暗号アルゴリズムＥＡＮＧでユーザＵ〔Ｂ〕と暗号化通信を実施するための鍵L_Bを生成し、平文データＭＤを＜デスクランブル機能確認終了＞と定める。

【０１５０】

次に、暗号アルゴリズムＥＡＮＧ及び鍵L_Bを、暗号アルゴリズムＥＢＦ及び鍵K_Bでそれぞれ暗号化して、暗号文EBF_{KB}（ＥＡＮＧ）及びEBF_{KB}（L_B）を作成する。

【０１５１】

さらに、平文データＭＤを暗号アルゴリズムＥＡＮＧ及び鍵L_Bで暗号化して、暗号文$EANG_{LB}$（ＭＤ）を作成する。前記３組の暗号文は、鍵管理ワークステーション５００のスクランブル機能５３０により作成される。

【０１５２】

この３組の暗号文を＜暗号アルゴリズム更新要求＞として、ユーザU〔B〕に配信する。

【０１５３】

４：　この３組の暗号文、EBF_{KB}（EANG）、EBF_{KB}（L_B）及びENG_{LB}（MD）を受け取ったユーザU〔B〕は、デスクランブル機能１４０によりこれらの暗号文を復号する。

【０１５４】

まず、鍵構成管理ＤＢ１８０に格納されている鍵K_Bより、暗号文EBF_{KB}（EANG）と暗号文EBF_{KB}（L_B）を復号し、暗号アルゴリズムＥＡＮＧ、及び鍵L_Bを取得する。

【０１５５】

暗号アルゴリズム管理機能１２０は、取得した暗号アルゴリズムＥＡＮＧを暗号アルゴリズムＤＢ１９０に格納するとともに、暗号アルゴリズムの運用状態を暗号アルゴリズムＥＢＦから、暗号アルゴリズムＥＡＮＧに更新する。また、鍵構成管理機能１１０は、取得した鍵L_Bを鍵構成管理ＤＢ１８０に格納する。

【０１５６】

このようにして、暗号アルゴリズム及び鍵が更新された。

【０１５７】

次に、更新された暗号アルゴリズムＥＡＮＧ及び鍵L_Bを用いて、暗号文ENG_{LB}（MD）を復号し、平文データＭＤを取得する。取得した平文データＭＤが＜デスクランブル機能確認終了＞となっていることを確認し、変換した暗号アルゴリズムＥＡＮＧによるデスクランブル機能１４０が正常に動作することを確認する。

【０１５８】

５：　次に、平文データＭＳを＜スクランブル機能確認終了＞とし、スクランブル機能１３０を動作させ暗号アルゴリズムＥＡＮＧ及び鍵L_Bを用いて暗号化し、暗号文$EANG_{LB}$（ＭＳ）を作成する。

【０１５９】

この作成した暗号文を＜暗号アルゴリズム更新報告＞として、鍵管理用ワークステーション５００に配信する。

【０１６０】

６：　＜暗号アルゴリズム更新報告＞を受信した鍵管理用ワークステーションは、暗号アルゴリズムＥＡＮＧ及び鍵L_Bを用いて復号化し、平文データＭＳを取得する。取得した平文データＭＳが＜スクランブル機能確認終了＞となっていることを確認し、ユーザＵ〔Ｂ〕の変換した暗号アルゴリズムＥＡＮＧによるスクランブル機能１３０が正常に動作することを確認する。これにより、暗号アルゴリズム変換と、暗号化、復号化を実施するスクランブル機能１３０、デスクランブル機能１４０とが正常に動作することが確認され、暗号アルゴリズム変換を終了する。

【０１６１】

７：　以上の手順により、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とは、同一の暗号アルゴリズムＥＡＮＧを共有することが可能となった。これより、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕との暗号化通信を再開し、鍵管理用ワークステーションはユーザＵ〔Ａ〕にアルゴリズムＥＡＮＧに基づいて＜セッション鍵発行＞を実施する。

【０１６２】

以上、暗号アルゴリズムの暗号化による配信と、運用する鍵の変換及び、変換した暗号アルゴリズムの動作確認の手順について説明した。

【０１６３】

以下に、アルゴリズム変換の詳細について説明する。ここでは、運用される暗号が公開鍵暗号か共通鍵暗号かについて着目し、暗号化通信システムが共通鍵暗号で構成されている場合の暗号アルゴリズム変換（本発明の第２の実施の形態）について説明し、次に、暗号化通信システムが公開鍵暗号で構成されている場合の暗号アルゴリズム変換（本発明の第３の実施の形態）について説明する。なお、これらの実施の形態において、基本的な構成は、上述した第１の実施の形態と同様であるので、以下の説明では、その相違点を中心にして、それぞれの場合の

暗号アルゴリズム変換の詳細について説明する。

【０１６４】

まず、図６から図１０を参照して、本発明の第２の実施の形態について説明する。ここでは、共通鍵暗号で構成されている暗号化通信システムにおける暗号アルゴリズム変換について説明する。すなわち。図１の暗号化通信システムにおいて、運用される暗号アルゴリズムＡ〔１〕～Ａ〔ｎ〕及びＢ〔１〕～Ｂ〔ｍ〕がすべて共通鍵暗号アルゴリズムである場合の暗号アルゴリズム変換について説明する。

【０１６５】

図５及び図７を参照して、共通鍵暗号アルゴリズムによる暗号化通信について説明する。

【０１６６】

暗号化通信を行う前提条件とし、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局よりユーザＩＤと、マスター鍵としての秘密鍵とが割り当てられており、鍵管理用ワークステーションのネットワーク鍵構成ＤＢに、ユーザに割り当てたマスター鍵をユーザＩＤと対応させて登録し管理しているものとする。同様に鍵管理局自身にもマスター鍵としての秘密鍵P_{CID}が割り当てられているものとする。

【０１６７】

本実施の形態では、データの暗号化に用いるスクランブル鍵k_sの暗号アルゴリズムと、デスクランブル鍵K_Dの配送に用いるセッション鍵の暗号アルゴリズムとを、異なった暗号アルゴリズムとする二重暗号化方式を取っており、同一の暗号アルゴリズムを使用する場合とくらべてセキュリティの向上を図っている。本実施例では、セッション鍵とマスター鍵を運用する暗号アルゴリズムは、同一の暗号アルゴリズムを使用することとしている。

【０１６８】

以下、ユーザＵ〔Ａ〕からユーザＵ〔Ｂ〕に暗号化通信を行う場合を例にして、暗号化通信の内容について説明する。

【０１６９】

（１）ユーザＵ〔Ａ〕からユーザＵ〔Ｂ〕に暗号化通信を行う場合、ユーザＵ〔Ａ〕は鍵管理局に、セッション鍵発行要求を行う。ここで、ユーザＵ〔Ａ〕は、送信側ユーザとし、ユーザＵ〔Ｂ〕は、受信側ユーザとする。このセッション鍵発行要求を受けて、鍵管理用ワークステーションのネットワーク暗号アルゴリズム管理機能は、ネットワーク暗号アルゴリズムＤＢの検索を行い、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とが使用している暗号アルゴリズムが同一かどうかの判断を行う。

【０１７０】

（２）ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とが同一の暗号アルゴリズムを使用していると判断したとき、鍵管理用ワークステーションのネットワーク鍵管理機能は、その暗号アルゴリズムでセッション鍵P_Tを生成する。次に、送信側のユーザのマスター鍵ＰＩＤ、受信側のユーザのマスター鍵P_{YID}をネットワーク鍵管理ＤＢより取り出し、セッション鍵P_Tを平文として暗号化を行い、暗号文$E_{PID}(P_T)$、$E_{PYID}(P_T)$を作成する。この暗号文を送信側ユーザの使用するパーソナルコンピュータなどの情報処理装置に送付する。

【０１７１】

（３）送信側のユーザが使用するパーソナルコンピュータでは、管理しているユーザのマスター鍵P_{ID}を鍵構成管理ＤＢより取り出し、この鍵を用いて、暗号化されて送付されたセッション鍵を復号し、セッション鍵P_Tを取得する。

【０１７２】

（４）一方、ユーザが入力したデータＭを受け取り、このデータＭを暗号化するためのスクランブル鍵k_S、復号化するためのデスクランブル鍵K_Dを生成する。

【０１７３】

（５）次に、ユーザが入力したデータＭをスクランブル鍵k_Sで暗号化し、暗号文$E_{ks}(M)$を作成し、同様にデスクランブル鍵K_Dをセッション鍵P_Tで暗号化し、暗号文$E_{PT}(k_D)$を作成する。この作成した２組の暗号文と、送付された暗号文$E_{PYID}(P_T)$とを送信先相手のユーザの使用するパーソナルコンピュ

ータなどの情報処理装置に送信する。

【０１７４】

（６）送信先相手ユーザ側のパーソナルコンピュータは、このユーザのマスター鍵P_{YID}を鍵構成管理ＤＢより取り出し，この鍵を用いて送付された暗号化セッション鍵E_{PYID}（P_T）を復号し、セッション鍵P_Tを取得する。次に送付された暗号化デスクランブル鍵E_{PT}（K_D）を取得したセッション鍵P_Tを用いて復号し、デスクランブル鍵K_Dを取得する。

【０１７５】

最後に、このデスクランブル鍵K_Dを用いて送付されたデータの暗号文E_{ks}（M）を復号し、データＭを取得する。

【０１７６】

鍵管理用ワークステーションのネットワーク暗号アルゴリズム管理機能がユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とが同一の暗号アルゴリズムを使用していないと判断すると、ユーザＵ〔Ｂ〕の暗号アルゴリズムの変換を実施し、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とが同一の暗号アルゴリズムを運用できるようにする。

【０１７７】

次に、図６及び図８、９を参照して、本実施の形態における暗号アルゴリズム変換の手順について説明する。

【０１７８】

（１）ネットワーク暗号アルゴリズム管理機能は、送信側のユーザから、送信側ユーザのユーザＩＤと送信先相手ユーザのユーザＩＤとを付加したセッション鍵発行要求を受けると、送付されたユーザＩＤをキーとして、ネットワーク暗号アルゴリズムＤＢの検索を実施し、送信側ユーザと送信先相手ユーザの運用する暗号アルゴリズムの状態を把握する。図７に示すように暗号化通信システムは共通鍵暗号による二重暗号方式をとっており、データの暗号化に用いる暗号アルゴリズムと、セッション鍵を運用する暗号アルゴリズムとの二種類の暗号アルゴリズムを用いている。送信側ユーザと送信先相手ユーザとが運用する二種類の暗号アルゴリズムが一致しないと、両者の間で暗号化通信を実施することはできない。

【０１７９】

ネットワーク暗号アルゴリズムＤＢを検索の結果、一致しない場合、送信側ユーザの運用する暗号アルゴリズムＥＡＮＧを取り出す。取り出した暗号アルゴリズムには、データの暗号化に用いるものか、セッション鍵の運用に用いるかの識別子を付加するものとする。当然、二種類の暗号アルゴリズムが一致しなければ、二種類の暗号アルゴリズムを取り出すことになる。

【０１８０】

送信先相手ユーザの運用している暗号アルゴリズムをＥＢＦとすると、この暗号アルゴリズムＥＢＦから取り出した暗号アルゴリズムＥＡＮＧに暗号アルゴリズムを変換させることになる。

【０１８１】

（２）鍵管理用ワークステーションのネットワーク鍵管理機能は、変換前の暗号アルゴリズムＥＢＦでセション鍵P_{TA}を生成し、変換後の暗号アルゴリズムＥＡＮＧでセション鍵P_{TB}を生成する。セッション鍵を運用するアルゴリズムに変更がなければ、P_{TA}及びP_{TB}は同一である。次に、送信先相手ユーザのユーザＩＤキーとして、ネットワーク鍵管理ＤＢを検索し、送信先相手ユーザのマスター鍵P_{YID}を取り出す。

【０１８２】

暗号アルゴリズムを変換した場合、暗号化通信に使用する鍵の鍵長すなわちビット数は、長くなったり、短くなったりする。従って、このような場合には、暗号鍵の鍵長の変更を暗号アルゴリズムの変換と併せて行うことが要求される。

【０１８３】

図１０を参照して、暗号アルゴリズムの変換に伴なう、暗号鍵の変換について説明する。

【０１８４】

鍵のビット数が短くなる場合は、図１０の（ａ）に示すように、送信先相手ユーザのマスター鍵P_{YID}及び、鍵管理局自身のマスター鍵P_{CID}の後ろの冗長分のビット数を削除し，新しく送信先相手ユーザのマスター鍵P_{YIDC}及び、鍵管理局自身のマスター鍵P_{CIDC}とする。

【０１８５】

一方、鍵のビット数が長くなる場合は、図１０の（ｂ）に示すように、不足分のビット数に合わせて乱数ＹＲ，ＣＲを生成し、P_{YID}に乱数ＹＲをつなげて，新しく送信先相手ユーザのマスター鍵P_{YIDC}（$P_{YIDC}=P_{YID}$ ‖ ＹＲ）とし、P_{CID}に乱数ＣＲをつなげて新しくネットワーク鍵管理用ワークステーション自身のマスター鍵P_{CIDC}（$C_{CIDC}=C_{CID}$ ‖ ＣＲ）とする。

【０１８６】

ここで、新しく更新したユーザのマスター鍵P_{YIDC}，P_{CIDC}は、ほかのユーザのマスター鍵と同一の可能性があるため、ネットワーク鍵管理ＤＢを検索し、同一のマスター鍵のユーザがいないことを確認し、また、同一のマスター鍵のユーザが存在する場合は、必要な鍵長で新しく生成するものとする。

【０１８７】

（３）変換前の暗号アルゴリズムＥＢＦを使用して以下の暗号文を作成する。

【０１８８】

１：　変換前の暗号アルゴリズムＥＢＦとマスター鍵P_{YID}でセッション鍵P_{TA}を暗号化し、暗号文EBF_{PYID}（P_{TA}）を作成する。

【０１８９】

２：　変換前の暗号アルゴリズムＥＢＦとセッション鍵P_{TA}で暗号アルゴリズムＥＡＮＧを暗号化し、暗号文EBF_{PTA}（ＥＡＮＧ）を作成する。

【０１９０】

３：　変換前の暗号アルゴリズムＥＢＦとセッション鍵P_{TA}で変換後の送信先相手ユーザのマスター鍵P_{YIDC}を暗号化し、暗号文EBF_{PTA}（P_{YIDC}）を作成する。当然、送信先相手ユーザのマスター鍵に変更がなければ、この暗号文は作成しない。

【０１９１】

（４）変換後の暗号アルゴリズムＥＡＮＧを使用して以下の暗号文を作成する。

【０１９２】

１：　変換後の暗号アルゴリズムＥＡＮＧと、変換後の送信先相手ユーザのマ

スター鍵P_{YIDC}とで変換後の暗号アルゴリズムで運用するセション鍵P_{TB}を暗号化し暗号文$EANG_{PYIDC}(P_{TB})$を作成する。

【０１９３】

当然、セッション鍵を運用する暗号アルゴリズムに変更がなければ、この暗号文は、$EBF_{PYID}(P_{TA})$と同じである。

【０１９４】

２：　変換後の暗号アルゴリズムＥＡＮＧと変換後の鍵管理用ワークステーション自身のマスター鍵P_{CIDC}で変換後の暗号アルゴリズムで運用するセション鍵P_{TB}を暗号化し暗号文$EANG_{PCIDC}(P_{TB})$を作成する。

【０１９５】

当然、セッション鍵を運用する暗号アルゴリズムに変更がなければ、この暗号文は、変換前の暗号アルゴリズムＥＢＦと変換前の鍵管理用ワークステーション自身のマスター鍵P_{CID}で変換前の暗号アルゴリズムで運用するセション鍵P_{TA}を暗号化して作成する暗号文$EBF_{PCID}(P_{TA})$と同じものになる。

【０１９６】

３：　平文データＭＤを＜アルゴリズム変換後のデスクランブル機能確認終了＞とする。

【０１９７】

変換後の暗号アルゴリズムＥＡＮＧでこの平文データＭＤを暗号化するためのスクランブル鍵k_{SC}、復号化するためのデスクランブル鍵K_{DC}を生成する。

【０１９８】

次に、データＭＤをスクランブル鍵k_{SC}で暗号化し、暗号文$E_{ksC}(MD)$を作成し、同様にデスクランブル鍵K_{DC}を変換後の暗号アルゴリズムで運用するセション鍵P_{TB}で暗号化し、暗号文$EANG_{PTB}(K_{DC})$を作成する。

【０１９９】

（５）前記（３）項で作成した３組の暗号文$EBF_{PYID}(P_{TA})$、EBF_{PTA}（ＥＡＮＧ）及び$EBF_{PTA}(P_{YIDC})$と、前記（４）で作成した４組の暗号文$EANG_{PYIDC}(P_{TB})$、$EANG_{PCIDC}(P_{TB})$、$E_{ksC}(MD)$及び$EANG_{PTB}(k_{DC})$とを＜暗号アルゴリズム変換要求＞として、送信先相手ユーザに送付

する。ここで、前記（３）項で作成した３組の暗号文は、送信先相手ユーザの暗号アルゴリズムを変換するための情報であり、前記（４）項で作成した４組の暗号文は、暗号アルゴリズムを変換後、変換した暗号アルゴリズムが正常に機能するか確認するための情報である。

【０２００】

（６）送信先相手ユーザの暗号アルゴリズムの変換、及びマスター鍵の更新

送信先相手ユーザは、暗号アルゴリズムとしてＥＢＦを運用しており、マスター鍵としてP_{YID}を所有している。鍵管理用ワークステーションより送付された暗号文から、

１：　マスター鍵としてP_{YID}を用いて、暗号文$EBF_{PYID}(P_{TA})$を復号し、セッション鍵P_{TA}を取得する。

【０２０１】

２：　セッション鍵P_{TA}を用いて暗号文EBF_{PTA}（ＥＡＮＧ）を復号し、暗号アルゴリズムＥＡＮＧを取得する。

【０２０２】

３：　セッション鍵P_{TA}を用いて暗号文$EBF_{PTA}(P_{YIDC})$を復号し、マスター鍵P_{YIDC}を取得する。

【０２０３】

以上のようにして、送信先相手ユーザは、暗号アルゴリズムＥＡＮＧとマスター鍵P_{YIDC}とを取得した。これより、取得した暗号アルゴリズムＥＡＮＧを暗号アルゴリズム管理ＤＢに登録するとともに、暗号アルゴリズム管理機能により運用する暗号アルゴリズムをＥＢＦからＥＡＮＧに変換する。

【０２０４】

送信先相手ユーザのマスター鍵が変更になる場合は、鍵構成管理機能によりマスター鍵をP_{YID}からP_{YIDC}に更新する。

【０２０５】

（７）送信先相手ユーザの変換された暗号アルゴリズムによるデスクランブル機能の確認

鍵管理用ワークステーションより送付された暗号文を、変換された暗号アルゴ

リズムのデスクランブル機能により復号しデスクランブル機能が正常に動作することを確認する。

【０２０６】

１：　マスター鍵としてP_{YIDC}を用いて、暗号文$EANG_{PYIDC}$（P_{TB}）を復号し、セッション鍵P_{TB}を取得する。

【０２０７】

２：　セッション鍵P_{TB}を用いて暗号文$EANG_{PTB}$（k_{DC}）を復号し、デスクランブル鍵k_{DC}を取得する。

【０２０８】

３：　デスクランブル鍵k_{DC}を用いて暗号文E_{ksc}（ＭＤ）を復号し、平文データＭＤを取得する。

【０２０９】

４：　平文データＭＤが＜アルゴリズム変換後のデスクランブル機能確認終了＞であることを確認し、デスクランブル機能が正常動作することを確認する。

【０２１０】

（８）送信先相手ユーザの変換された暗号アルゴリズムによるスクランブル機能の駆動

変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認するため、平文データを設定し、スクランブル機能で暗号化し鍵管理用ワークステーションに送付する。

【０２１１】

１：　平文データＭＳを＜アルゴリズム変換確認試験終了＞とする。変換後の暗号アルゴリズムＥＡＮＧでこの平文データＭＳを暗号化するためのスクランブル鍵K_{su}、復号化するためのデスクランブル鍵K_{du}を生成する。次に、データＭＳをスクランブル鍵k_{Su}で暗号化し、暗号文$EANG_{ksu}$（ＭＳ）を作成し、同様にデスクランブル鍵K_{du}を取得したセション鍵P_{TB}で暗号化し、暗号文$EANG_{PTB}$（k_{Du}）を作成する。

【０２１２】

２：　作成した２組の暗号文$EANG_{PTB}$（k_{DU}）及び$EANG_{ksu}$（ＭＳ）と

、鍵管理用ワークステーションから送付された暗号文ＥＡＮＧ$_{PCIDC}$（Ｐ$_{TB}$）とを鍵管理用ワークステーションに＜暗号アルゴリズム変換確認要求＞として返送する。

【０２１３】

（９）鍵管理用ワークステーションでの暗号アルゴリズム変換の確認

送信先相手ユーザから返送された暗号文を復号し、送信先相手ユーザの変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【０２１４】

１：　鍵管理用ワークステーションのマスター鍵Ｐ$_{CIDC}$を用いて、暗号文ＥＡＮＧ$_{PCIDC}$（Ｐ$_{TB}$）を復号し、セッション鍵Ｐ$_{TB}$を取得する。

【０２１５】

２：　セッション鍵Ｐ$_{TB}$を用いて暗号文ＥＡＮＧ$_{PTB}$（Ｋ$_{DU}$）を復号し、デスクランブル鍵Ｋ$_{DU}$を取得する。

【０２１６】

３：　デスクランブル鍵ｋ$_{Du}$を用いて暗号文Ｅ$_{ksu}$（ＭＳ）を復号し、平文データＭＳを取得する。

【０２１７】

４：　取得した平文データＭＳが＜アルゴリズム変換確認試験終了＞であることを確認し、送信先相手ユーザのスクランブル機能が正常動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【０２１８】

このようにして、共通鍵暗号が運用されるネットワーク通信システムにおいて、アルゴリズム変換を実施することができる。

【０２１９】

このアルゴリズム変換により、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とは、同一の暗号アルゴリズムを共有することになった。これにより、図７に示す手順により、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とは暗号化通信を実施することが可能となった。

【０２２０】

本実施の形態において、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とが、同一系列の暗号強度が同じか、または異なる暗号アルゴリズムを所有している場合は、ネットワーク暗号アルゴリズム管理機能により強度の強い暗号アルゴリズムに変換することも可能である。

【０２２１】

この場合、ユーザＵ〔Ａ〕のほうがユーザＵ〔Ｂ〕より強い強度の暗号アルゴリズムをもっている場合は、ユーザＵ〔Ｂ〕をユーザＵ〔Ａ〕の暗号アルゴリズムに変換することになり、逆に、ユーザＵ〔Ｂ〕のほうが強ければ、ユーザＵ〔Ａ〕をユーザＵ〔Ｂ〕の暗号アルゴリズムに変換することになる。

【０２２２】

このアルゴリズム変換は、図６及び図８，９に示す手順と同様にして実行することができる。

【０２２３】

次に、鍵管理用ワークステーションが管理している暗号アルゴリズムの暗号強度を上げるか、または、暗号強度は変えずに暗号アルゴリズムのバージョンを変えてセキュリティを改善する例について示す。

【０２２４】

図１で示したように、暗号アルゴリズムＡ〔１〕～Ａ〔ｎ〕は、同一のＡ暗号系列の鍵管理用ワークステーションが管理している暗号アルゴリズムであり、鍵管理用ワークステーションはこの暗号のアルゴリズムを生成する機能を有している。暗号アルゴリズムを変更することにより、暗号強度を変えたり、暗号化演算の手順を変えることができ、同一の暗号アルゴリズムを使用することと比較すると、暗号化通信システムのセキュリティを改善することができる。

【０２２５】

同一のＡ系列の暗号アルゴリズムを運用するユーザのユーザＩＤは、Ｕ〔Ａｉ，ｊ〕であり、鍵管理用ワークステーションは、このユーザのなかから暗号アルゴリズムを変更するユーザを定める。そして、暗号のアルゴリズムを生成する機能を用いて、新しく暗号アルゴリズムを生成し、暗号アルゴリズムを変更すると

定めたユーザに新しく生成した暗号アルゴリズムを配信する。

【０２２６】

この配信は、前述した暗号アルゴリズムのアルゴリズム変換と同様にして行うことができる。

【０２２７】

以上で、バージョンが異なる暗号アルゴリズム、暗号強度が異なる暗号アルゴリズムを配信する例について説明した。

【０２２８】

各ユーザに配信された暗号アルゴリズムに各ユーザの暗号アルゴリズムは変換されるわけであるが、変換前の暗号アルゴリズムは、消さないで各ユーザの暗号アルゴリズムＤＢに格納するようにし、鍵管理用ワークステーションは、各ユーザが暗号アルゴリズムＤＢに格納されている暗号アルゴリズムを、ネットワーク暗号アルゴリズム管理ＤＢに管理するようにしておく。

【０２２９】

このようにしておくと、ユーザＵ〔Ａ〕からユーザＵ〔Ｂ〕に暗号化通信要求が生じた場合、双方のユーザの暗号アルゴリズムＤＢに共通の暗号アルゴリズムが存在する場合は、鍵管理用ワークステーションが暗号アルゴリズムを配信する必要はなく、鍵管理用ワークステーションがこの共通の暗号アルゴリズムへ切り替えの指示を出せば、ユーザＵ〔Ａ〕からユーザＵ〔Ｂ〕に暗号化通信が可能となる。

【０２３０】

以上、暗号化通信システムが共通鍵暗号で構成されている場合の暗号アルゴリズム変換のについて説明した。

【０２３１】

次に、図１１から図１５を参照して、本発明の第３の実施の形態について説明する。ここでは、公開鍵暗号が運用されるネットワーク通信システム、すなわち、暗号化通信システムが公開鍵暗号で構成されている場合の暗号アルゴリズム変換について説明する。

【０２３２】

図１に示すネットワーク通信システムにおいて、運用される暗号アルゴリズムＡ〔１〕～Ａ〔ｎ〕及びＢ〔１〕～Ｂ〔ｍ〕は、すべて公開鍵暗号アルゴリズムとする。

【０２３３】

図１２を参照して、公開鍵暗号アルゴリズムによる暗号化通信について説明する。

【０２３４】

公開鍵暗号アルゴリズムとしては、例えば、楕円曲線暗号の暗号アルゴリズムを適用することができる。この楕円曲線暗号の鍵の演算を記載するのに必要な楕円曲線のベースポイントをＰとする。楕円曲線暗号については、例えば、信学技報 TECNICAL REPORT OF IEICE ISEC 97-15(1997-07)「楕円曲線を利用した高速暗号化法」宝木和夫、車谷博之に記載されている。

【０２３５】

暗号化通信を実施する場合、鍵管理用ワークステーションのネットワーク鍵管理機能からセッション鍵の発行を受け、この鍵をもとに受け取ったデータを暗号化し暗号文を作成し、送信先相手ユーザ側のパーソナルコンピュータのデスクランブル機能に送信する。

【０２３６】

デスクランブル機能は、送付された暗号文を復号化し、データを取得する。

【０２３７】

暗号化通信処理部を運用する前提条件として、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理用ワークステーションより、ユーザＩＤとマスター鍵として、秘密鍵d_{ID}と、この秘密鍵に対応する公開鍵Q_{ID}（$＝P・d_{ID}$；・は楕円曲線上の演算）とを割り当てられており、鍵管理用ワークステーションのネットワーク鍵管理ＤＢに、ユーザに割り当てた公開鍵Q_{ID}をユーザＩＤと対応させて登録し管理している。同様に、鍵管理用ワークステーション自身にも、マスター鍵として、秘密鍵d_Cと、この秘密鍵に対応する公開鍵Q_C（$＝P・d_C$；・は楕円曲線上の演算）が割り当てられているものとし、鍵管理

用ワークステーション自身の公開鍵Q_Cは、本システムを利用するすべてのユーザに公開するものとする。

【０２３８】

本実施例では、データの暗号化をスクランブル鍵K_Sで行い、データの復号化をデスクランブル鍵K_Dで行うものとし、このデスクランブル鍵K_Dの配送を公開鍵暗号である楕円曲線暗号で実施するものとする。スクランブル鍵K_S，デスクランブル鍵K_Dを運用する共通鍵暗号アルゴリズムとしては、例えば、ＭＵＬＴＩ２暗号アルゴリズムを用いることができる。ＭＵＬＴＩ２暗号アルゴリズムは、ＣＳデジタル放送などで実績がある暗号アルゴリズムである。

【０２３９】

以下、ユーザＵ〔Ａ〕からユーザＵ〔Ｂ〕に暗号化通信を行う場合を例にとって説明する。ここで、ユーザＵ〔Ａ〕は送信側ユーザとし、ユーザＵ〔Ｂ〕は受信側ユーザとする。

【０２４０】

（１）ユーザＵ〔Ａ〕からユーザＵ〔Ｂ〕に暗号化通信を行う場合、ユーザＵ〔Ａ〕は鍵管理用ワークステーションに、セッション鍵発行要求を行う。このセッション鍵発行要求を受けて、鍵管理用ワークステーションのネットワーク暗号アルゴリズム管理機能は、ネットワーク暗号アルゴリズムＤＢの検索を行い、ユーザＵ〔Ａ〕が使用している暗号アルゴリズムと、ユーザＵ〔Ｂ〕が使用している暗号アルゴリズムとが同一かどうかの判断を行う。

【０２４１】

（２）ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とが同一の暗号アルゴリズムを使用していると判断したとき、鍵管理用ワークステーションのネットワーク鍵管理機能は、ユーザＩＤをキーとしてネットワーク鍵管理ＤＢを検索し、送信先相手ユーザのマスター鍵に対応する公開鍵Q_{YID}と、送信側ユーザのマスター鍵に対応する公開鍵Q_{ID}とを取り出す。

【０２４２】

取り出した公開鍵Q_{YID}と公開鍵Q_{ID}とに対して、鍵管理用ワークステーションのマスター鍵である秘密鍵d_Cで署名作成演算を実施し署名データS_{dc}（Q_{YID}

）と署名データＳｄｃ（Q_{ID}）とを作成する。この公開鍵Q_{YID}をセッション鍵とし署名データS_{dc}（Q_{YID}）及び署名データS_{dc}（Q_{ID}）とを組み合わせて、送信側ユーザに送付しセッション鍵の発行を実施する。

【０２４３】

（３）公開鍵Q_{YID}と署名データS_{dc}（Q_{YID}）及び署名データS_{dc}（Q_{ID}）を受信したユーザは、鍵管理用ワークステーションの公開鍵Q_Cを用いて署名データS_{dc}（Q_{YID}）とQ_{YID}とに対し署名検証演算を実施し、公開鍵Q_{YID}が正当な鍵管理用ワークステーションから送付されたものであることを確認し、通信しようとする正当な送信先相手ユーザに割り当てられた公開鍵であることを確認する。

【０２４４】

このようにして、送信側ユーザはセッション鍵として使用する公開鍵の発行を受ける。

【０２４５】

（４）送信側のユーザは、送信するデータＭを暗号化するためのスクランブル鍵K_Sと復号するためのデスクランブル鍵K_Dを生成する。

【０２４６】

次にユーザの入力するデータＭをスクランブル鍵K_Sで暗号化し、暗号文E_{Ks}（Ｍ）を作成する。

【０２４７】

また、送付されたセッション鍵としての公開鍵Q_{YID}でデスクランブル鍵K_Dを暗号化し、暗号化デスクランブル鍵E_{QYID}（K_D）を生成する。

【０２４８】

また、送信するデータＭが確実に送信側ユーザが作成したものであることを保証するため、鍵管理用ワークステーションより送信側ユーザに割り当てられているマスター鍵としての秘密鍵d_{ID}で、送信するデータＭに署名作成演算を実施し、署名データS_{dID}（Ｍ）を作成する。

【０２４９】

公開鍵暗号の場合、送付された鍵Q_{YID}は、そのまま暗号化のための鍵として

使用することができる。

【０２５０】

このようにして作成した２組の暗号文E_{Ks}（M）及びE_{QYID}（K_D）と、データMに関する署名データS_{dID}（M）と、鍵管理用ワークステーションより送付された送信側ユーザの公開鍵に関する署名データS_{dc}（Q_{ID}）及び送信側ユーザ自身の公開鍵Q_{ID}との５組のデータを送信相手先のユーザに送信する。

【０２５１】

（５）５組のデータを受信した送信相手先のユーザは、まず鍵管理用ワークステーションの公開鍵Ｑｃを用いて署名データS_{dc}（Q_{ID}）及びQ_{ID}に対し署名検証演算を実施し、公開鍵Q_{ID}が正当な鍵管理用ワークステーションから送付されたものであることを確認し、正当な送信側ユーザに割り当てられた公開鍵であることを確認する。

【０２５２】

鍵管理用ワークステーションより送信相手先のユーザに割り当てられているマスター鍵としての秘密鍵d_{YID}で、暗号化デスクランブル鍵E_{QYID}（K_D）を復号し、デスクランブル鍵K_Dを取得する。

【０２５３】

次に、このデスクランブル鍵K_Dを用いて、暗号文E_{Ks}（M）を復号し、データMを得る。

【０２５４】

最後に、送信側ユーザから送付された公開鍵Q_{ID}を用いて署名データS_{dID}（M）とデータMとに対し署名検証演算を実施し、データMが正当な送信側ユーザから伝達されたデータであることを確認する。

【０２５５】

このようにして、ネットワーク通信システムにおいて、ユーザU〔A〕からユーザU〔B〕に対して暗号化通信を行うことが可能となる。

【０２５６】

一方、暗号アルゴリズム管理機能がユーザU〔A〕とユーザU〔B〕とが同一の暗号アルゴリズムを使用していないと判断すると、ユーザU〔B〕の暗号アル

ゴリズムの変換を実施し、ユーザU〔A〕とユーザU〔B〕とが同一の暗号アルゴリズムを運用できるようにする。

【０２５７】

以下、図１１及び図１３，１４を参照して、公開鍵暗号アルゴリズムが運用されるネットワーク通信システムにおける暗号アルゴリズム変換について説明する。

【０２５８】

（１）ネットワーク暗号アルゴリズム管理機能は、送信側のユーザから、送信側ユーザのユーザＩＤと送信先相手ユーザのユーザＩＤとを付加したセッション鍵発行要求を受けると、送付されたユーザＩＤをキーとしてネットワーク暗号アルゴリズム管理ＤＢの検索を実施し、送信側ユーザと送信先相手ユーザが運用する暗号アルゴリズムの状態を把握する。図１１に示すようにネットワーク通信システムは、二重暗号方式の暗号化通信システムをとっており、データの暗号化に共通鍵暗号アルゴリズムを用い、セッション鍵の運用に公開鍵の暗号アルゴリズムを用いている。

【０２５９】

送信側ユーザと送信先相手ユーザとが運用する二種類の暗号アルゴリズムが一致しないと、両者の間で暗号化通信を実施することはできない。

【０２６０】

ネットワーク暗号アルゴリズム管理ＤＢを検索の結果、一致しない場合、送信側ユーザの運用する暗号アルゴリズムＥＡＮＧを取り出す。取り出した暗号アルゴリズムには、データの暗号化に用いるものか、セッション鍵の運用に用いるかの識別子を付加するものとする。当然、二種類の暗号アルゴリズムが両方一致しなければ、二種類の暗号アルゴリズムを取り出すことになる。

【０２６１】

送信先相手ユーザの運用している暗号アルゴリズムをＥＢＦとすると、この暗号アルゴリズムＥＢＦから取り出した暗号アルゴリズムＥＡＮＧに暗号アルゴリズムを変換させることになる。

【０２６２】

（２）鍵管理用ワークステーションのネットワーク鍵管理機能は、ユーザＩＤをキーとしてネットワーク鍵管理ＤＢを検索し変換前の暗号アルゴリズムＥＢＦの送信先相手ユーザのマスター鍵に対応する公開鍵Q_{YID}を取り出す。

【０２６３】

暗号アルゴリズムＥＡＮＧに変換された場合、送信先相手ユーザの変換前の暗号アルゴリズムＥＢＦでのマスター鍵が使用できなくなる場合がある。この場合、ネットワーク鍵管理機能は暗号アルゴリズムの変換に対して送信先相手ユーザのマスター鍵に互換性があるか無いかの判断を行い、互換性が無いと判断した場合は、新規に送信先相手ユーザの公開鍵を生成する。

【０２６４】

新しく生成したマスター鍵としての秘密鍵をd_{YIDC}としこの秘密鍵に対応する公開鍵をQ_{YIDC}とする。

【０２６５】

鍵管理用ワークステーションは、変換前の暗号アルゴリズムＥＢＦ、及び、変換後の暗号アルゴリズムＥＡＮＧのどちらの暗号アルゴリズムに対しても対応するマスター鍵が割り当てられている。

【０２６６】

変換前の暗号アルゴリズムＥＢＦに対応するマスター鍵としての秘密鍵をd_Cとしこの秘密鍵に対応する公開鍵をQ_Cとする。

【０２６７】

変換後の暗号アルゴリズムＥＡＮＧに適応するマスター鍵としての秘密鍵をd_{CG}としこの秘密鍵に対応する公開鍵をQ_{CG}とする。

【０２６８】

（３）ネットワーク鍵管理機能は，変換前の暗号アルゴリズムＥＢＦを使用して、以下の暗号文及び、署名データを作成する。

【０２６９】

１：　変換前の暗号アルゴリズムＥＢＦで暗号アルゴリズムＥＡＮＧ及び秘密鍵d_{YIDC}を暗号化するためのスクランブル鍵K_{SB}、復号化するためのデスクラン

ブル鍵K_{DB}を生成する。

【０２７０】

２：　暗号アルゴリズムＥＡＮＧ及び秘密鍵d_{YIDC}をスクランブル鍵k_{SB}で暗号化し、暗号文EBF_{KSB}（ＥＡＮＧ）と暗号文EBF_{KSB}（d_{YIDC}）を作成する。また、取り出したマスター鍵としての公開鍵Q_{YID}でデスクランブル鍵K_{DB}を暗号化し、暗号文EBF_{QYID}（K_{DB}）を作成する。

【０２７１】

３：　変換前の暗号アルゴリズムＥＢＦと鍵管理用ワークステーションのマスター鍵である秘密鍵d_cで、新しく生成した秘密鍵d_{YIDC}と公開鍵Q_{YIDC}とに対し署名作成演算を実施し、署名データＳｄｃ（d_{YIDC}）及び署名データS_{dc}（Q_{YIDC}）を作成する。

【０２７２】

４：　変換前の暗号アルゴリズムＥＢＦと鍵管理用ワークステーションのマスター鍵である秘密鍵d_cで、暗号アルゴリズムＥＡＮＧに対し署名作成演算を実施し、署名データS_{dc}（ＥＡＮＧ）を作成する。

【０２７３】

５：　変換前の暗号アルゴリズムＥＢＦと鍵管理用ワークステーションのマスター鍵である秘密鍵d_cで、変換後の暗号アルゴリズムＥＡＮＧに適用する鍵管理用ワークステーションのマスター鍵としての公開鍵Q_{CG}に対して署名作成演算を実施し、署名データS_{dc}（Q_{CG}）を作成する。

【０２７４】

（４）スクランブル機能は，変換後の暗号アルゴリズムＥＡＮＧを使用して、以下の暗号文及び、署名データを作成する。

【０２７５】

１：　平文データＭＤを＜アルゴリズム変換後のデスクランブル機能確認終了＞とする。

【０２７６】

変換後の暗号アルゴリズムＥＡＮＧで、前記平文データＭＤを暗号化するためのスクランブル鍵K_{SC}、復号化するためのデスクランブル鍵K_{DC}を生成する。次

にデータＭＤをスクランブル鍵Ｋｓｃで暗号化し、暗号文$EANG_{KSC}$（ＭＤ）を作成し、同様にデスクランブル鍵K_{DC}を変換後の暗号アルゴリズムで運用するセション鍵として運用する公開鍵Q_{YIDC}で暗号化し、暗号文$EANG_{QYIDC}$（k_{DC}）を作成する。

【０２７７】

２：　変換後の暗号アルゴリズムＥＡＮＧで鍵管理用ワークステーションのマスター鍵とし割り当てられている秘密鍵d_{cg}で、新しく生成した公開鍵Q_{YIDC}と、平文データＭＤとに対して署名作成演算を実施し、署名データS_{dcg}（Q_{YIDC}），S_{dcg}（ＭＤ）を作成する。

【０２７８】

（５）前記（３）項で作成した３組の暗号文EBF_{QYID}（K_{DB}）、EBF_{KSB}（ＥＡＮＧ）及びEBF_{KSB}（d_{YIDC}）と、４組の署名データS_{dc}（d_{YIDC}）、S_{dc}（Q_{YIDC}）、S_{dc}（ＥＡＮＧ）及びS_{dc}（Q_{CG}）と、新しく生成した公開鍵Q_{YIDC}と、鍵管理用ワークステーションの公開鍵Q_{CG}と、前記（４）項で作成した２組の暗号文$EANG_{KSC}$（ＭＤ）及び$EANG_{QYIDC}$（K_{DC}）並びに２組の署名データS_{dcg}（Q_{YIDC}），S_{dcg}（ＭＤ）とを＜暗号アルゴリズム変換要求＞として送信先相手ユーザに送付する。ここで、前記（３）項で作成した暗号文及び署名データは、送信先相手ユーザの暗号アルゴリズムを変換するための情報であり、前記（４）項で作成した４組の暗号文及び署名データは、暗号アルゴリズムを変換後、変換した暗号アルゴリズムが正常に機能するか確認するための情報である。

【０２７９】

ネットワーク鍵管理機能は、新しく生成した送信先相手ユーザのマスター鍵としての公開鍵Q_{YIDC}をネットワーク鍵管理ＤＢに暗号アルゴリズムＥＡＮＧと対応させて格納する。

【０２８０】

（６）送信先相手ユーザの暗号アルゴリズムの変換、及びマスター鍵の更新

送信先相手ユーザは、暗号アルゴリズムとしてＥＢＦを運用しており、マスター鍵としての秘密鍵d_{YID}、及び暗号アルゴリズムＥＢＦで運用される鍵管理用

ワークステーションの公開鍵Q_Cを所有している。

【０２８１】

鍵管理用ワークステーションより送付された暗号文から、

１：　マスター鍵として秘密鍵d_{YID}を用いて、暗号文EBF_{QYID}（K_{DB}）を復号し、デスクランブル鍵K_{DB}を取得する。次にこのデスクランブル鍵K_{DB}を用いて暗号文EBF_{KSB}（ＥＡＮＧ）を復号し、暗号アルゴリズムＥＡＮＧを取得する。鍵管理用ワークステーションの公開鍵Q_Cを用いて、署名データS_{dc}（ＥＡＮＧ）と、取得した暗号アルゴリズムＥＡＮＧとに対して署名検証演算を実施し、取得した暗号アルゴリズムＥＡＮＧが正当な鍵管理用ワークステーションから送付されたものであることを確認する。

【０２８２】

２：　デスクランブル鍵K_{DB}を用いて、暗号文EBF_{KSB}（d_{YIDC}）を復号し、変換した暗号アルゴリズムＥＡＮＧ上で運用する、当該ユーザのマスター鍵として秘密鍵d_{YIDC}を取得する。

【０２８３】

鍵管理用ワークステーションの公開鍵Q_Cを用いて、署名データS_{dc}（d_{YIDC}）と、取得した秘密鍵d_{YIDC}とに対して署名検証演算を実施し、取得した取得した秘密鍵d_{YIDC}が正当な鍵管理用ワークステーションから送付されたものであることを確認する。同様に、鍵管理用ワークステーションの公開鍵Q_Cを用いて、署名データS_{dc}（Q_{YIDC}）と、送付されたマスター鍵である公開鍵Q_{YIDC}とに対して署名検証演算を実施し、取得した取得した公開鍵Q_{YIDC}が正当な鍵管理用ワークステーションから送付されたものであることを確認する。

【０２８４】

３：　鍵管理用ワークステーションの公開鍵Q_Cを用いて、署名データS_{dc}（Q_{CG}）と、送付された鍵管理用ワークステーションの変換した暗号アルゴリズムＥＡＮＧ上で運用する公開鍵Q_{CG}とに対して署名検証演算を実施し、送付された公開鍵Q_{CG}が正当な鍵管理用ワークステーションの公開鍵であることを確認する。

【０２８５】

以上のようにして、送信先相手ユーザは、暗号アルゴリズムＥＡＮＧと、マスター鍵としての秘密鍵d_{YIDC}と、この秘密鍵に対応する公開鍵Q_{YIDC}と、鍵管理用ワークステーションの変換した暗号アルゴリズムＥＡＮＧ上で運用する公開鍵Q_{CG}とを取得した。これらにより、取得した暗号アルゴリズムＥＡＮＧを暗号アルゴリズム管理ＤＢに登録するとともに、暗号アルゴリズム管理機能によって運用する暗号アルゴリズムを、暗号アルゴリズムＥＢＦから暗号アルゴリズムＥＡＮＧに変換する。

【０２８６】

送信先相手ユーザのマスター鍵が変更になる場合は、鍵構成管理機能によりマスター鍵としての秘密鍵をd_{YID}からd_{YIDC}に更新する。

【０２８７】

（７）送信先相手ユーザの変換された暗号アルゴリズムによるデスクランブル機能の確認

鍵管理用ワークステーションより送付された暗号文を、変換された暗号アルゴリズムのデスクランブル機能により復号しデスクランブル機能が正常に動作することを確認する。

【０２８８】

１：　マスター鍵として秘密鍵d_{YIDC}を用いて、暗号文$EANG_{QYIDC}$（K_{DC}）を復号し、デスクランブル鍵K_{DC}を取得する。

【０２８９】

２：　デスクランブル鍵K_{DC}を用いて暗号文$EANG_{KSC}$（ＭＤ）を復号し、平文データＭＤを取得する。次に、鍵管理用ワークステーションの公開鍵Q_{CG}を用いて、署名データS_{dcg}（ＭＤ）と取得した平文データＭＤとに対して署名検証演算を実施し、取得した平文データＭＤが正当な鍵管理用ワークステーションから送付されたものであることを確認する。

【０２９０】

３：　平文データＭＤが＜アルゴリズム変換後のデスクランブル機能確認終了＞であることを確認し、デスクランブル機能が正常動作することを確認する。

【０２９１】

（８）送信先相手ユーザの変換された暗号アルゴリズムによるスクランブル機能の駆動

変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認するため、平文データを設定し、スクランブル機能で暗号化し鍵管理用ワークステーションに送付する。

【０２９２】

１：　平文データＭＳを＜アルゴリズム変換確認試験終了＞とする。変換後の暗号アルゴリズムＥＡＮＧで前記平文データＭＳを暗号化するためのスクランブル鍵K_{SU}及び復号化するためのデスクランブル鍵K_{DU}を生成する。次に、平文データＭＳをスクランブル鍵K_{SU}で暗号化し、暗号文$EANG_{KSU}$（ＭＳ）を作成し、同様に、デスクランブル鍵K_{DU}を鍵管理用ワークステーションの公開鍵Q_{CG}で暗号化し、暗号文$EANG_{QCG}$（K_{DU}）を作成する。また、データＭＳに対して送信先相手ユーザのマスター鍵としての秘密鍵d_{YIDC}を用いて署名作成演算を実施し、署名データS_{dYIDC}（ＭＳ）を作成する。

【０２９３】

２：　作成した２組の暗号文$EANG_{QCG}$（K_{DU}）及び$EANG_{KSU}$（ＭＳ）と、署名データS_{dYIDC}（ＭＳ）と、鍵管理用ワークステーションから送付された署名データS_{dcg}（Q_{YIDC}）と、送信先相手ユーザの公開鍵Q_{YIDC}とを＜暗号アルゴリズム変換確認要求＞として鍵管理用ワークステーションに返送する。

【０２９４】

（９）鍵管理用ワークステーションでの暗号アルゴリズム変換の確認

送信先相手ユーザから返送された暗号文を復号し、送信先相手ユーザの変換された暗号アルゴリズムのスクランブル機能が正常に動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【０２９５】

１：　鍵管理用ワークステーションのマスター鍵としての秘密鍵d_{cg}を用いて、暗号文$EANG_{QCG}$（K_{DU}）を復号し、デスクランブル鍵K_{DU}を取得する。

【０２９６】

２：　デスクランブル鍵K_{DU}を用いて暗号文ＥＡＮＧ$_{ksu}$（ＭＳ）を復号し、平文データＭＳを取得する。

【０２９７】

３：　鍵管理用ワークステーションの公開鍵Q_{cg}を用いて、署名データS_{dcg}（Q_{YIDC}）と送付された送信先相手ユーザの公開鍵Q_{YIDC}とに対して署名検証演算を実施し、付された送信先相手ユーザの公開鍵Q_{YIDC}が正当な送信先相手ユーザ、すなわち受信側ユーザから送付されたものであることを確認する。

【０２９８】

４：　送信先相手ユーザの公開鍵Q_{YIDC}を用いて、署名データS_{dYIDC}（ＭＳ）と取得した平文データＭＳとに対して署名検証演算を実施し、取得した平文データＭＳが正当な送信先相手ユーザ、すなわち受信側ユーザから送付されたものであることを確認する。

【０２９９】

５：　取得した平文データＭＳが＜アルゴリズム変換確認試験終了＞であることを確認し、送信先相手ユーザのスクランブル機能が正常動作することを確認し、これにより変換後の暗号アルゴリズムが正常に動作することを確認する。

【０３００】

以上の（１）～（９）により、本実施の形態におけるアルゴリズム変換の実施例について示した。この暗号アルゴリズム変換により、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕とは、同一の暗号アルゴリズムを共有することになった。これにより、図１２に示されるようにして、ユーザＵ〔Ａ〕とユーザＵ〔Ｂ〕との間で暗号化通信を実施することが可能となった。

【０３０１】

暗号アルゴリズムを変換した場合、本実施例では、ユーザの所有するマスター鍵としての秘密鍵と、この秘密鍵に対応する公開鍵とを、鍵管理用ワークステーションで新しく生成している。

【０３０２】

これらの鍵は、全く新しく生成してもよいが、変換前の鍵をもとに生成するこ

とも可能である。以下、この鍵の生成について説明する。

【０３０３】

公開鍵暗号の場合も暗号化通信に使用する秘密鍵は、共通鍵暗号の場合と同様、暗号アルゴリズム変換により、秘密鍵の鍵長すなわちビット数は、長くなったり、短くなったりする。

【０３０４】

鍵のビット数が短くなる場合は、送信先相手ユーザの変換前のマスター鍵としての秘密鍵d_{YID}の後ろの冗長分のビット数を削除し，これを新しく送信先相手ユーザのマスター鍵としての秘密鍵d_{YIDC}とする。

【０３０５】

鍵のビット数が長くなる場合は、図１５に示すように、不足分のビット数に合わせて乱数ＹＲを生成し、d_{PYID}にＹＲをつないで，新しく送信先相手ユーザのマスター鍵としての秘密鍵d_{YIDC}（$d_{YIDC}=P_{YID} \parallel$ ＹＲ）とする。

【０３０６】

生成した秘密鍵d_{YIDC}に対応して公開鍵Q_{YIDC}（$=P \cdot d_{YIDC}$；・は楕円曲線上の演算）が定まる。

【０３０７】

この公開鍵Q_{YIDC}が、以前に生成した他のユーザの秘密鍵になっている可能性もあるため、鍵管理用ワークステーションは、ネットワーク暗号アルゴリズム管理ＤＢを検索し、同じ公開鍵がないことを確認する。もし同じ公開鍵が存在するようならば、再度乱数を生成しマスター鍵としての秘密鍵を生成する。

【０３０８】

ここで、ＹＲとして、常に０の値を使用することも可能である。

【０３０９】

マスター鍵，セッション鍵を運用する暗号アルゴリズムは、前述のように共通鍵暗号アルゴリズムとは異なる楕円曲線暗号アルゴリズムを用いており、これにより、二重暗号方式が構成され、セキュリティの向上が図られている。

【０３１０】

次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲

線暗号を用いた場合の鍵管理部について説明する。公開鍵暗号を用いた場合の鍵管理部のソフト機能は、図２に示す共通鍵暗号の場合のソフト機能と同じである。前述の公開鍵暗号アルゴリズムを使用した場合の暗号化処理部、及びアクセス管理部のソフト機能構成の実施例に示すように、各ユーザのマスター鍵は秘密鍵d_{ID}であり、この秘密鍵と楕円曲線上の演算で公開鍵Q_{ID}（$=d_{ID}\cdot P$；・は楕円曲線上の演算）が対応している。また、スクランブル鍵及びデスクランブル鍵の暗号アルゴリズムは、共通鍵暗号アルゴリズムとしてＭＵＬＴＩ２暗号アルゴリズムとしている。

【０３１１】

次に、本発明の第４の実施の形態について説明する。ここでは、可搬型の情報処理装置に組み込まれている暗号機能における暗号アルゴリズムの変換について説明する。

【０３１２】

上述の第１から第３の実施の形態においては、図１に示すように複数の暗号アルゴリズムがネットワーク通信システムに存在し、鍵管理用ワークステーションが各ユーザの暗号アルゴリズムの状態を把握し、暗号化通信の要求が発生するごとに、必要に応じてこの鍵管理用ワークステーションが各ユーザの暗号アルゴリズムを変換し、ユーザ間の暗号化通信を実施するようにしている場合について説明した。

【０３１３】

上述の説明では、図１に示すように複数の暗号アルゴリズムがネットワーク通信システムに存在し、鍵管理局用ワークステーションが各ユーザの暗号アルゴリズムの状態を把握し、暗号化通信の要求が発生するごとに、必要に応じてこの鍵管理局用ワークステーションが各ユーザの暗号アルゴリズムを変換し、ユーザ間の暗号化通信を実施するようにしている。

【０３１４】

ところが、近年、可搬型の情報処理装置、例えば、携帯端末装置、ＩＣカードなどに、暗号機能が組み込まれ、電子マネーなどの自動支払いなどに使用されるようになった。

【０３１５】

すなわち、ユーザは、暗号機能が組み込まれた情報処理装置としてのＩＣカードを所有し、電子マネーなどを自動支払いする場合、このＩＣカードを店舗等に設置された情報処理装置としての読取り機にさし込み、両者の情報処理によって、支払いなどの決済を行う。

【０３１６】

この場合、ＩＣカードが鍵管理局用ワークステーションと接続して、暗号処理を実施するのは、ユーザの手続きが煩雑となり、不便である。

【０３１７】

以下、可搬型の情報処理装置（端末、ＩＣカードなど）で運用される暗号アルゴリズム変換に好適な暗号アルゴリズム変換方式について説明する。

【０３１８】

図１２に示す、公開鍵暗号アルゴリズムで運用される暗号化通信システムにおいて、暗号化通信を実施する際、図２で示したように、送信側ユーザは、鍵管理用ワークステーションに＜セッション鍵発行要求＞を行い、該鍵管理用ワークステーションから、送信先相手ユーザの公開鍵Q_{YID}及び該公開鍵$_{YID}$の署名データS_{dc}（Q_{YID}）と、自分自身の公開鍵Q_{ID}及び該公開鍵Q_{ID}の署名データS_{dc}（Q_{ID}）との発行を受ける。

【０３１９】

ここで、各自の公開鍵Q_{ID}及び署名データS_{dc}（Q_{ID}）とを各ユーザが鍵構成管理ＤＢに格納するようにしておく。すなわち、公開鍵暗号アルゴリズムで運用される暗号化通信システムを図１６に示す方式（該方式を機能ブロック図で表すと図２５のようになる）とし、各ユーザが自分自身の公開鍵Q_{ID}及び該公開鍵Q_{ID}の署名データS_{dc}（Q_{ID}）を、予め鍵管理用ワークステーションから、図１６における点線で示すルートで配布されて受け取り、各ユーザの鍵構成管理ＤＢに所有するようにしておけば、暗号化通信を実施する際の＜セッション鍵発行要求＞を鍵管理用ワークステーションにするのではなく、送信先相手ユーザにすることができる。

【０３２０】

すなわち、＜セッション鍵発行要求＞を送信先相手ユーザに送付し、送信先相手ユーザから相手ユーザの公開鍵Q_{YID}と、この公開鍵の署名データS_{dc}（Q_{YID}）との送付をうける。

【０３２１】

図１６に示す方式において、各ユーザに割り当てるマスター鍵としての秘密鍵d_{ID}は、鍵管理用ワークステーションが生成する方式と、各ユーザが生成する方式とが考えられる。

【０３２２】

１：　鍵管理用ワークステーションが生成する方式

マスター鍵としての秘密鍵d_{ID}及び対応する公開鍵Q_{ID}を鍵管理用ワークステーションが生成してくれれば、暗号アルゴリズムの運用に不慣れなユーザにとっては非常に便利である。

【０３２３】

しかし、各ユーザにどのようにして生成した秘密鍵を配布するかが問題となる。

【０３２４】

本実施の形態では、ＩＣカードやフロッピーディスクなどの電子媒体に格納し、ユーザに確実に配布することにする。

【０３２５】

生成した秘密鍵d_{ID}を鍵管理用ワークステーションが保持することにすると、ユーザが対応する公開鍵Q_{ID}で暗号化するデータを鍵管理用ワークステーションがすべて解読することが可能となる。このように、鍵管理用ワークステーションが、ユーザの情報を握ることを防止するため、本実施の形態では、生成した秘密鍵d_{ID}に鍵回復機能を持たせ、ネットワーク鍵構成ＤＢに、ユーザＩＤと対応させて保存するようにし、不測の事態以外は、ユーザが作成した暗号文を解読できないようにする。

【０３２６】

以下に、本実施の形態における鍵回復機能について、鍵が二重の階層構造を有

する暗号化通信を例にとって説明する。鍵回復機能は、暗号文E_{KS}（M）に解読の情報を付加し、デスクランブル鍵K_Dによらずに暗号文を解読する手段を与えるものである。

【０３２７】

まず、次に、共通鍵暗号アルゴリズムによる暗号化通信における鍵回復機能について説明する。すなわち、ユーザが送信するデータをMとし、可搬型の情報処理装置が生成するスクランブル鍵K_Sによりデータは暗号化され、暗号文E_{KS}（M）が作成される。この暗号文を復号するためのデスクランブル鍵K_Dを、鍵管理用ワークステーションから送付されたセッション鍵P_Tによって暗号化し、暗号文E_{PT}（K_D）を作成している。

【０３２８】

まず、図２３を参照して、スクランブル鍵K_Sでデータを暗号化する際、鍵回復機能を持たせるための付加データの作成手順について説明する。

【０３２９】

（１）スクランブル鍵K_Sを生成するとき、乱数を生成しＫ１，Ｋ２の排他的論理和（ＸＯＲ、図では、直和記号で示している。）により、スクランブル鍵をK_S＝　Ｋ１　ＸＯＲ　Ｋ２と表現できるようにする。

【０３３０】

（２）Ｐ１，Ｐ２を鍵回復用の鍵とし、可搬型の情報処理装置及び、鍵管理用ワークステーションの鍵回復機能で保管するものとする。スクランブル鍵K_Sを生成するときに生成したＫ１，Ｋ２をこの鍵回復用の鍵Ｐ１，Ｐ２で暗号化して暗号文E_{P1}（Ｋ１）、E_{P2}（Ｋ２）を作成する。このデータを、スクランブル鍵K_Sで作成したデータの暗号文E_{KS}（M）に付加するものとする。

【０３３１】

次に、図２４を参照して、この付加データで暗号文を復号する手順について説明する。

【０３３２】

（１）暗号文から付加されたデータE_{P1}（Ｋ１）、E_{P2}（Ｋ２）を分離し、鍵回復用の鍵Ｐ１，Ｐ２でＫ１，Ｋ２を復号する。

【０３３３】

（２）Ｋ１，Ｋ２の排他的論理和を取り、K_S＝　Ｋ１　ＸＯＲ　Ｋ２として、スクランブル鍵K_Sを生成する。共通鍵暗号の場合、スクランブル鍵K_Sとデスクランブル鍵K_Dとは同一であり、このスクランブル鍵K_Sにより、暗号文を復号することができる。

【０３３４】

不測の事態が発生して、暗号文を解読する必要が生じた場合、暗号文を鍵管理用ワークステーションに送付すれば、前記に示した手順により、鍵回復用の鍵Ｐ１，Ｐ２を用いて暗号文を解読することができる。

【０３３５】

次に、公開鍵暗号アルゴリズムによる暗号化通信における鍵回復機能について説明する。すなわち、データＭの暗号化に用いるスクランブル鍵をK_S，デスクランブル鍵をK_Dとし、デスクランブル鍵を配送するためのセッション鍵としての公開鍵をQ_{YID}とすると、暗号化通信は、暗号文E_{KS}（Ｍ）と暗号化デスクランブル鍵E_{QYID}（K_D）の送信により実施される。

【０３３６】

ここでは、公開鍵暗号として楕円曲線暗号を用いられる場合を例にとって説明する。楕円曲線暗号については、例えば、信学技報　ＴＥＣＮＩＣＡＬ　ＲＥＰＯＲＴ　ＯＦ　ＩＥＩＣＥ　ＩＳＥＣ９７－１５（１９９７－０７）の「楕円曲線を利用した高速暗号化方法」　宝木和夫，車谷博之に記載されている。

【０３３７】

まず、暗号化デスクランブル鍵E_{QYID}（K_D）にしきい値ロジックを付加する鍵回復機能について説明する。

【０３３８】

（１）鍵管理用ワークステーションの鍵回復機能において、鍵回復用の公開鍵Q_A，Q_B，Q_Cを割り当て、公開するとともに、この公開鍵に対応する秘密鍵d_A，d_B，d_C（$Q_A=d_A\cdot P$，$Q_B=d_B\cdot P$，$Q_C=d_C\cdot P$）を保管するものとする。

【０３３９】

暗号化デスクランブル鍵E_{QYID}（K_D）には、鍵Q_{YID}，Q_A，Q_B，Q_Cで算出されるしきい値ロジックを付加するものとする。

【０３４０】

（２）共通鍵暗号を用いた場合と同様、暗号化通信を行う場合、デスクランブル鍵K_Dを暗号化してからでないと、データをスクランブル鍵K_Sで暗号化できないようにし、データの暗号文E_{KS}（M）と暗号化デスクランブル鍵E_{QYID}（K_D）は必ずペアで生成されるようにする。

【０３４１】

（３）不測の事態が発生して暗号文を解読する必要が生じた場合、ペアとなった暗号文E_{KS}（M），E_{QYID}（K_D）を鍵管理ワークステーションに送付する。

【０３４２】

鍵回復機能では、秘密鍵d_A，d_B，d_Cの２つと、E_{QYID}（K_D）に付加されたしきい値ロジックを用いて復号し、デスクランブル鍵K_Dを取得する。

【０３４３】

次に、この鍵K_Dで暗号文E_{KS}（M）を復号し、データMを取得する。

【０３４４】

ここで、送信するデータMの暗号文は、スクランブル鍵K_Sによる暗号化演算で作成される。このため、共通鍵暗号を用いた鍵回復機能（暗号化について図２３、復号化について図２４参照）と全く同様に、スクランブル鍵K_SをＫ１，Ｋ２の排他的論理和で表現し、これを用いて鍵回復を実施する方法をとることもできる。図２３、図２４に示す鍵回復用の鍵Ｐ１，Ｐ２は、共通鍵暗号アルゴリズムで運用することもできるが、鍵回復用として、公開鍵Q_A，Q_Bにより運用することも可能である。

【０３４５】

この場合暗号文E_{KS}（M）に鍵回復用として付加するデータは、Ｋ１，Ｋ２を公開鍵Q_A，Q_Bにより暗号化した暗号文E_{QA}（Ｋ１），E_{QB}（Ｋ２）であり、鍵回復は、鍵管理用ワークステーションの鍵回復機能において公開鍵Q_A，Q_Bに対応する秘密鍵d_A，d_Bを用いて、付加されたデータを復号することにより実施す

る。

【０３４６】

２：　各ユーザが生成する方式

暗号アルゴリズムの運用に慣れているユーザは、自分自身が使用するマスター鍵としての秘密鍵d_{ID}　及び対応する公開鍵Q_{ID}を自ら生成することも可能である。

【０３４７】

この場合、ユーザが所有するマスター鍵としての秘密鍵d_{ID}は、当該ユーザのみが所有するため、公開鍵Q_{ID}で作成した暗号文を鍵管理用ワークステーションから解読される可能性は、まったくない。

【０３４８】

当該ユーザは、秘密鍵d_{ID}に対応して生成した公開鍵Q_{ID}を鍵管理用ワークステーションに送付する。

【０３４９】

鍵管理用ワークステーションは、公開鍵Q_{ID}を送付した当該ユーザの身元を確認し、送付された公開鍵Q_{ID}に、鍵管理用ワークステーションの所有する秘密鍵d_cにより署名作成演算を実施し、署名データS_{dc}（Q_{ID}）を当該ユーザに送付する。

【０３５０】

本実施の形態では、１：項で示した場合と同様、ユーザの所有するマスター鍵としての秘密鍵d_{ID}は、鍵回復機能を持たせ、ネットワーク鍵構成ＤＢに、ユーザＩＤと対応させて保存するようにする。

【０３５１】

各ユーザが所有するマスター鍵としての秘密鍵d_{ID}及び、対応する公開鍵Q_{ID}を鍵管理用ワークステーションが生成するか、ユーザが生成するかは、ユーザの事情に応じて、ユーザが選択するものとする。

【０３５２】

以上のような方式をとることにより、ＩＣカードと店舗等に設置された情報処理装置としての読取り機とは、鍵管理用ワークステーションを経由せず、ＩＣカ

ードを店舗等に設置された情報処理装置としての読取り機に挿し込んだ状態で暗号化通信を実施することができる。

【０３５３】

ユーザがＩＣカードを情報処理装置としての読取り機に挿し込んだ時、ＩＣカードと報処理装置としての読取り機の暗号アルゴリズムが異なる場合、両者の暗号アルゴリズムを同一にしなければ、暗号化通信、すなわち支払いなどの決済を実施することができない。

【０３５４】

この場合、暗号アルゴリズム変換を実施する必要が生じるが、ＩＣカードを店舗等に設置された情報処理装置としての読取り機にさし込んだままこの暗号アルゴリズム変換が実施できれば、ユーザの手続きは簡便となり便利である。

【０３５５】

図１７，図１８を参照して、このような暗号アルゴリズム変換について説明する。

【０３５６】

暗号としては、前述の楕円曲線暗号とする。楕円曲線暗号の場合、楕円曲線$Y^2=X^3+ax+b$の係数ａ及びｂと、係数の標数ｐと、ベースポイントＰ及びその位数ｎとで暗号アルゴリズムが定まりる。この暗号アルゴリズムは、秘匿してもよいし、また、公開してもよい。

【０３５７】

楕円曲線暗号の公開鍵Ｑと秘密鍵ｄとは、ベースポイントＰにより、Ｑ＝ｄ・Ｐ（・は、楕円曲線上の演算）と表される。

【０３５８】

楕円曲線$y^2=x^3+ax+b$の係数ａ，ｂが同じでも、ベースポイントＰを変更することにより、同じ暗号強度の別の暗号アルゴリズムを与えることができる。係数ａ，ｂおよび係数の標数ｐを変更すると、楕円曲線が変わり、別の暗号アルゴリズムが定まる。

【０３５９】

係数ａ，ｂおよび係数の標数ｐの変更の前後で、同程度の鍵長となるように、

楕円曲線を生成すれば、同程度の、暗号強度の相異なる複数の暗号アルゴリズムを与えることができる。

【０３６０】

係数ａ，ｂおよび係数の標数ｐを変更する場合、楕円曲線の生成法によっては、暗号強度、すなわち鍵長を変更することも可能である。

【０３６１】

以下、ＩＣカードが使用している暗号アルゴリズムをＥＢＦ、情報処理装置としての読取り機の使用している暗号アルゴリズムをＥＡＮＧとし、ＥＢＦの鍵長よりもＥＡＮＧの鍵長のほうが長いと仮定した場合を例にとって、暗号アルゴリズム変換の実施態様について説明する。

【０３６２】

ここで、図２１を参照して、暗号アルゴリズム変換の対象とする暗号化通信システムについて説明する。この暗号化通信システムは、暗号鍵が一重の階層構造をとっている。すなわち、図１６示される暗号化通信システムでのスクランブル鍵と、デスクランブル鍵とを運用せずに暗号化通信システムが構築している。

【０３６３】

まず、図３のネットワーク通信システムのソフト機能を参照し、送信側ユーザ、受信側ユーザ、及びネットワーク管理用ワークステーションがそれぞれ所有している、鍵と暗号アルゴリズムに関するＤＢについて説明する。本実施の形態では、送信側ユーザが情報処理装置としての読取り機に対応し、また、受信側ユーザがＩＣカードなどの可搬型の情報処理装置に対応している。

【０３６４】

図１９を参照して、この鍵と暗号アルゴリズムに関するＤＢに格納される情報の具体例について説明する。

【０３６５】

（１）鍵管理用ワークステーションのＤＢについて

１：　ネットワーク暗号アルゴリズム管理ＤＢ

本ネットワーク通信システムで使用するすべての楕円曲線の暗号アルゴリズムＡ〔１〕，Ａ〔２〕，…，Ａ〔Ｎ〕と、各暗号アルゴリズムに対応するバージョ

ン番号V_B〔1〕，V_B〔2〕，…，V_B〔N〕と、この暗号アルゴリズムに対して鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_C〔1〕，d_C〔2〕，…，d_C〔N〕と、この秘密鍵に対応する公開鍵Q_C〔1〕，Q_C〔2〕，…，Q_C〔N〕とをおのおの対応させて格納するものとする。

【０３６６】

特に、本実施の形態における暗号アルゴリズムＥＢＦには、バージョン番号をＢＦ，マスター鍵としての秘密鍵をd_C、この秘密鍵に対応する公開鍵をQ_Cとし、暗号アルゴリズムＥＢＦに対応させて格納し、同様に本実施例の暗号アルゴリズムＥＡＮＧには、バージョン番号をＢＧ，マスター鍵としての秘密鍵をd_{cg}、この秘密鍵に対応する公開鍵をQ_{cg}とし、暗号アルゴリズムＥＡＮＧに対応させて格納するものとする。

【０３６７】

２：　ネットワーク鍵管理ＤＢ

各ユーザ、すなわちＩＣカード及び情報処理装置としての読取り機のユーザＩＤをＩＤ〔1〕，ＩＤ〔2〕，…，ＩＤ〔M〕とし、このユーザが使用する暗号アルゴリズムのバージョン番号を、V_{BP}〔1〕，V_{BP}〔2〕，…，V_{BP}〔M〕とし、この暗号アルゴリズムで各ユーザが使用する公開鍵を、Q_{ID}〔1〕，Q_{ID}〔2〕，…，Q_{ID}〔M〕とし、各々をユーザＩＤに対応させて格納するものとする。

【０３６８】

各ユーザが暗号アルゴリズムにあわせて使用するマスター鍵としての秘密鍵d_{ID}〔1〕，d_{ID}〔2〕，…，d_{ID}〔M〕は、鍵回復機能を持たせ、各ユーザＩＤに対応させて格納するものとする。

【０３６９】

（２）送信側ユーザ（情報処理装置としての読取り機）のＤＢについて

１：　暗号アルゴリズムＤＢ

（ｉ）　このユーザが運用している暗号アルゴリズムの情報として

暗号アルゴリズムＥＡＮＧ、バージョン番号ＢＧ、この暗号アルゴリズムのもとで鍵管理用ワークステーションが使用している公開鍵Q_{cg}、及び、暗号アルゴ

リズムＥＡＮＧに対する鍵管理用ワークステーションの署名データS_{dcg}（ＥＡＮＧ）を格納するものとする。

【０３７０】

ここで、署名データS_{dcg}（ＥＡＮＧ）は、暗号アルゴリズムＥＡＮＧのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_{cg}で暗号アルゴリズムＥＡＮＧに対して署名作成演算を実施したものである。

【０３７１】

（ｉｉ）　ネットワーク通信システムに運用されている暗号アルゴリズムの情報として、

暗号アルゴリズムＡ〔１〕，Ａ〔２〕，…，Ａ〔Ｎ〕、対応するバージョン番号V_B〔１〕，V_B〔２〕，…，V_B〔Ｎ〕、鍵管理用ワークステーションが使用する公開鍵Q_C〔１〕，Q_C〔２〕，…，Q_C〔Ｎ〕及び公開鍵Q_{cg}に対する鍵管理用ワークステーションの署名データS_{dc}〔１〕（Q_{cg}），S_{dc}〔２〕（Q_{cg}），…，S_{dc}〔Ｎ〕（Q_{cg}）をそれぞれ暗号アルゴリズムに対応させて格納するものとする。

【０３７２】

ここで、署名データS_{dc}〔ｉ〕（Q_{cg}）は、暗号アルゴリズムＡ〔ｉ〕のもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_C〔ｉ〕で公開鍵Q_{cg}に対して署名作成演算を実施したものである。

【０３７３】

特に、本実施例の暗号アルゴリズムＥＢＦには、バージョン番号をＢＦ，公開鍵Q_c及び、署名データS_{dc}（Q_{cg}）が暗号アルゴリズムＥＢＦに対応させて格納している。

【０３７４】

ここで、署名データS_{dc}（Q_{cg}）は、暗号アルゴリズムＥＢＦのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_cで公開鍵Q_{cg}に対して署名作成演算を実施したものである。

【０３７５】

２：　鍵構成管理ＤＢ

ユーザが運用する暗号アルゴリズム、すなわち本実施の形態では、暗号アルゴリズムＥＡＮＧのもとでユーザが使用するスター鍵としての秘密鍵d_{ID}とこの秘密鍵に対応する公開鍵Q_{ID}及びこの暗号アルゴリズムＥＡＮＧのもとで、鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_{cg}で公開鍵Q_{ID}に対して署名作成演算を実施することによって得られた署名データS_{dcg}（Q_{ID}）を格納するものとする。

【０３７６】

（３）受信側ユーザ（ＩＣカード）のＤＢについて

１：　暗号アルゴリズムＤＢ

このユーザが運用している暗号アルゴリズムの情報として

暗号アルゴリズムＥＢＦ，バージョン番号ＢＦ，この暗号アルゴリズムのもとで鍵管理用ワークステーションが使用している公開鍵Q_c及び、暗号アルゴリズムＥＢＦに対する鍵管理用ワークステーションの署名データS_{dc}（ＥＢＦ）を格納するものとする。

【０３７７】

ここで、署名データS_{dc}（ＥＢＦ）は、暗号アルゴリズムＥＢＦのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_cで暗号アルゴリズムＥＢＦに対して署名作成演算を実施したものである。

【０３７８】

２：　鍵構成管理ＤＢ

ユーザが運用する暗号アルゴリズム、すなわち本実施例では、暗号アルゴリズムＥＢＦのもとでユーザが使用するスター鍵としての秘密鍵d_{YID}とこの秘密鍵に対応する公開鍵Q_{YID}及びこの暗号アルゴリズムＥＢＦのもとで、鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_cで公開鍵Q_{YID}に対して署名作成演算を実施することによって得られた署名データS_{dc}（Q_{YID}）を格納するものとする。

【０３７９】

以上、暗号アルゴリズム変換の前提条件となる、鍵と暗号アルゴリズムに関するＤＢについて示した。

【０３８０】

送信側ユーザ、及び受信側ユーザのＤＢ（データベース）には、鍵管理用ワークステーションが使用する公開鍵、鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵で作成された署名データ、及び、暗号アルゴリズムとこれに対応するバージョン番号が格納されている。

【０３８１】

これらのデータは、すべて鍵管理用ワークステーションが配布するものとする。

【０３８２】

次に、図１７及び図１８を参照し、送信側ユーザ（情報処理装置としての読取り機）及び、受信側ユーザ（ＩＣカード）間で実施される暗号アルゴリズム変換の形態について説明する。

【０３８３】

暗号アルゴリズム変換に際して、楕円曲線の暗号アルゴリズムは公開して送付することも可能であるが、本実施例では、暗号化して送付するものとして説明する。

【０３８４】

ここでは、前にも述べたように鍵長がＥＢＦよりＥＡＮＧのほうがが長いものとし、ＩＣカードの暗号アルゴリズムＥＢＦを暗号アルゴズムＥＡＮＧに変換する場合の実施形態について示すこととする。

【０３８５】

１：　ＩＣカードを所有しているユーザは、店舗等で買い物を実施し、物品に対する支払いを行うため、ＩＣカードを情報処理装置としての読取り機に差し込む。

【０３８６】

情報処理装置としての読取り機の暗号化通信管理機能は、運用している暗号アルゴリズムＥＡＮＧに、バージョン番号ＢＧを付加して＜セッション鍵発行要求＞をＩＣカードの暗号化通信管理機能に送付する。

【０３８７】

２：　ＩＣカードの運用している暗号アルゴリズムのバージョン番号が、ＢＧと一致すれば、ＩＣカードは、自分の所有している公開鍵とこの公開鍵の署名データの発行を実施し、図２１に示す手順に従って情報処理装置としての読取り機との間で暗号化通信を実施する。

【０３８８】

しかし、ＩＣカードの運用している暗号アルゴリズムＥＢＦのバージョン番号は、ＢＦであり、送付されたバージョン番号ＢＧとは異なる。

【０３８９】

バージョン番号が異なると判断した暗号化通信管理機能は、このバージョン番号はＢＦを付加して、＜暗号アルゴリズム更新要求＞を情報処理装置としての読取り機の暗号化通信管理機能に返送する。

【０３９０】

３：　情報処理装置としての読取り機は、バージョン番号はＢＦをもとに暗号アルゴリズムＤＢを検索し、暗号アルゴリズムＥＡＮＧで運用する鍵管理用ワークステーションの公開鍵Q_{cg}及び、暗号アルゴリズムＥＢＦのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_cで公開鍵Q_{cg}に対して署名作成演算を実施して得られた署名データS_{dc}（Q_{cg}）とを取り出し、この公開鍵Q_{cg}と署名データS_{dc}（Q_{cg}）をＩＣカードに送付する。

【０３９１】

４：　ＩＣカードは、暗号アルゴリズムＥＢＦのもとに運用する鍵管理用ワークステーションの公開鍵Q_cを用いて、送付された公開鍵Q_{cg}と署名データS_{dc}（Q_{cg}）に対して署名検証演算を実施し、公開鍵Q_{cg}が正当な情報処理装置としての読取り機から送付されたものであることを確認する。

【０３９２】

５：　次に、ＩＣカードは、鍵構成管理ＤＢから暗号アルゴリズムＥＢＦで運用するＩＣカードの公開鍵Q_{YID}及び、暗号アルゴリズムＥＢＦのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_cで公開鍵Q_{YID}に対して署名作成演算を実施し，管理用ワークステーションから配布された署名デ

ータS_{dc}（Q_{YID}）とを取り出し、この公開鍵Q_{YID}と署名データS_{dc}（Q_{YID}）とを情報処理装置としての読取り機に送付する。

【０３９３】

６：　情報処理装置としての読取り機は、暗号アルゴリズムＥＢＦのもとに運用する鍵管理用ワークステーションの公開鍵Q_cを用いて、送付された公開鍵Q_{YID}と署名データS_{dc}（Q_{YID}）に対して署名検証演算を実施し、公開鍵Q_{YID}が正当なＩＣカードから送付されたものであることを確認する。

【０３９４】

７：　情報処理装置としての読取り機は、暗号アルゴリズムＥＡＮＧを送付された公開鍵Q_{YID}で暗号アルゴリズムＥＢＦを運用して暗号化し、暗号文$EBF_{Q_{YID}}$（ＥＡＮＧ）を作成する。

【０３９５】

これと併せて、暗号アルゴリズムＥＡＮＧのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_{cg}で暗号アルゴリズムＥＡＮＧに対して署名作成演算を実施し管理用ワークステーションから配布された署名データS_{dcg}（ＥＡＮＧ）を取り出し，暗号文EBF_{QYID}（ＥＡＮＧ）と署名データS_{dcg}（ＥＡＮＧ）とを、ＩＣカードに送付する。

【０３９６】

８：　ＩＣカードは、暗号アルゴリズムＥＢＦで運用するＩＣカード所有の秘密鍵d_{YID}を用いて送付された暗号文EBF_{QYID}（ＥＡＮＧ）を復号化し、暗号アルゴリズムＥＡＮＧを取得する。

【０３９７】

次に、ＩＣカードは、運用する暗号アルゴリズムをＥＢＦから取得したＥＡＮＧに変換し、４：項で取得した鍵管理ワークステーションの公開鍵Q_{cg}を用いて、取得した暗号アルゴリズムＥＡＮＧと送付された署名データS_{dcg}（ＥＡＮＧ）に対して、署名検証演算を実施し、正当な情報処理装置としての読取り機から配布された暗号アルゴリズムであることを確認する。これにより、暗号アルゴリズムをこのＥＡＮＧへの更新を完了する。

【０３９８】

９：　暗号アルゴリズムＥＡＮＧの鍵長は、暗号アルゴリズムＥＢＦより長いため、ＩＣカードのマスター鍵としての秘密鍵d_{YID}は、そのまま暗号アルゴリズムＥＡＮＧ　の秘密鍵として使用することとし、送付された暗号アルゴリズムＥＡＮＧのベースポイントＰより、対応する公開鍵Q_{YIDC}（＝Ｐ・d_{YID}；・は楕円曲線上の演算）を生成する。

【０３９９】

ＩＣカードは、暗号アルゴリズムを一旦ＥＢＦに戻し、この暗号アルゴリズムＥＢＦのもとに公開鍵Q_{YIDC}に対して秘密鍵d_{YID}を用いて署名作成演算を実施し、署名データS_{dYID}（Q_{YIDC}）を作成する。

【０４００】

ＩＣカードは、生成した公開鍵Q_{YIDC}及び署名データS_{dYID}（Q_{YIDC}）とを、情報処理装置としての読取り機に送付する。

【０４０１】

１０：　情報処理装置としての読取り機は、暗号アルゴリズムを一旦ＥＢＦに変換し、６：項で取得した公開鍵Q_{YID}を用いて、送付された署名データS_{dYID}（Q_{YIDC}）と公開鍵Q_{YIDC}に対して署名検証演算を実施し、正当なＩＣカードから配布されたＩＣカードの公開鍵Q_{YIDC}であることを確認する。

【０４０２】

この後、暗号アルゴリズムを再度暗号アルゴリズムＥＡＮＧに変換する。

【０４０３】

１１：　情報処理装置としての読取り機は、鍵構成管理ＤＢから暗号アルゴリズムＥＡＮＧで運用する情報処理装置としての読取り機の使用する公開鍵Q_{ID}及び、暗号アルゴリズムＥＡＮＧのもとに鍵管理用ワークステーションが使用するマスター鍵としての秘密鍵d_{cg}で公開鍵Q_{ID}に対して署名作成演算を実施し、管理用ワークステーションから配布された署名データS_{dcg}（Q_{ID}）とを取り出し、この公開鍵Q_{ID}と署名データS_{dcg}（Q_{ID}）とをＩＣカードに送付する。

【０４０４】

１２：　ＩＣカードは、暗号アルゴリズムＥＡＮＧのもと４：項で取得した鍵

管理用ワークステーションの公開鍵Q_{cg}を用いて、送付された署名データS_{dcg}（Q_{ID}）と公開鍵Q_{ID}に対して署名検証演算を実施し、正当な情報処理装置としての読取り機から送付された情報処理装置としての読取り機の公開鍵Q_{ID}であることを確認する。

【０４０５】

１３：　以上により、ＩＣカードと情報処理装置としての読取り機は、暗号アルゴリズムＥＡＮＧを共有し、お互いの公開鍵（情報処理装置としての読取り機の公開鍵Q_{ID}、及び、ＩＣカードの公開鍵Q_{YIDC}）の正当性を確認した。データの暗号化をこの公開鍵で実施することにすれば、ＩＣカードと情報処理装置としての読取り機との間で暗号化通信及び、署名作成演算、署名検証演算を実施することができ、支払いなどの決済が実施可能となった。

【０４０６】

ここで、上述した実施手順において、鍵管理用ワークステーションは一切関与していない。

【０４０７】

ただし、ＩＣカードは、変換した公開鍵Q_{YIDC}について、鍵管理用ワークステーションの署名データを所有していないため、これをそのまま使用することはできず、支払いなどの決済が終了したあと、暗号アルゴリズムをＥＡＮＧからＥＢＦに戻す必要がある。

【０４０８】

次に、図１８を参照し，ＩＣカードの変換した公開鍵Q_{YIDC}について、鍵管理用ワークステーションの署名データを取得する実施形態について説明する。

【０４０９】

１：　情報処理装置としての読取り機は、正当性を確認した暗号アルゴリズムＥＡＮＧで運用するＩＣカードの公開鍵Q_{YIDC}に対して、暗号アルゴリズムＥＢＦのもとに秘密鍵d_{YID}を用いて作成した署名データS_{dYID}（Q_{YIDC}）をＩＣカードから送られている。

【０４１０】

この署名データS_{dYID}（Q_{YIDC}）と公開鍵Q_{YIDC}、及び暗号アルゴリズムＥＢ

Ｆで運用するＩＣカードの公開鍵Q_{YID}、暗号アルゴリズムＥＢＦのバージョン番号ＢＦ，暗号アルゴリズムＥＡＮＧのバージョン番号ＢＧ及びＩＣカードのユーザＩＤとを鍵管理用ワークステーションに送付する。

【０４１１】

２：　鍵管理用ワークステーションは、まずＩＣカードのユーザＩＤをキーとして、ネットワーク鍵管理ＤＢを検索し、送付されたＩＣカードの公開鍵Q_{YID}が存在することを確認する。

【０４１２】

ＩＣカードの公開鍵Q_{YID}を用いて、署名データS_{dYID}（Q_{YIDC}）と公開鍵Q_{YIDC}に対して署名検証演算を実施し公開鍵Q_{YIDC}が正当なＩＣカードのものであることを確認する。

【０４１３】

以上により、公開鍵Q_{YIDC}が、ＩＣカードの公開鍵であることを確認した。

【０４１４】

３：　この公開鍵Q_{YIDC}に対して、暗号アルゴリズムＥＡＮＧで運用する鍵管理用ワークステーションの秘密鍵d_{cg}を用いて、署名作成演算を実施し、署名データS_{dcg}（Q_{YIDC}）を作成し、情報処理装置としての読取り機に返送する。

【０４１５】

また、鍵管理用ワークステーションは、ネットワーク鍵管理ＤＢのＩＣカードのユーザＩＤに対応させて格納している暗号アルゴリズムのバージョン番号及び公開鍵を、それぞれＢＧ及びQ_{YIDC}に更新する。

【０４１６】

４：　情報処理装置としての読取り機は、この署名データS_{dcg}（Q_{YIDC}）をＩＣカードに転送する。

【０４１７】

以上の処理を実施すれば、ＩＣカードは、公開鍵Q_{YIDC}に対して鍵管理用ワークステーションの署名データS_{dcg}（Q_{YIDC}）を取得することができる。

【０４１８】

上述した実施の形態において、鍵管理用ワークステーションは、変換前の公開

鍵Q_{YID}の存在と、変換御の公開鍵Q_{YIDC}の署名データを確認しており、ＩＣカードの成りすましを防止することができる。

【０４１９】

このようにして、ＩＣカードは暗号アルゴリズムＥＡＮＧで運用する公開鍵Q_{YIDC}と、鍵管理用ワークステーションの署名データS_{dcg}（Q_{YIDC}）とを所有し、以降暗号アルゴリズムＥＡＮＧを運用することが、可能となった。

【０４２０】

鍵管理用ワークステーションの関与は、変換した暗号アルゴリズムに対して生成された公開鍵について署名作成及び、署名検証演算の実施するだけであり、以上の方法によりＩＣカードを情報処理装置としての読取り機にさし込んだまま、暗号アルゴリズム変換を実施することができる。

【０４２１】

ここで示した、暗号アルゴリズム変換では、新しい暗号アルゴリズムに対して、ユーザ（ここではＩＣカード）は自分の所有する秘密鍵と公開鍵とを自ら生成している。

【０４２２】

ここで示した実施形態では、変換前の暗号アルゴリズムと変換後の暗号アルゴリズムに対して、ユーザの所有する秘密鍵を同一となるように定めている。

【０４２３】

このような秘密鍵の設定の方式は、システムに混在する複数の暗号アルゴリズムの鍵長がまちまちで、どのユーザがどの鍵長の暗号アルゴリズムを使用しているか特定できないときに有効である。

【０４２４】

これに対して、暗号アルゴリズム変換をすべてのユーザが使用していない、別の長い鍵長への変換を考える。

【０４２５】

この場合、各ユーザが使用する秘密鍵の鍵長を変換前のものと同じ鍵長で使用したとすれば、暗号アルゴリズムの許容する鍵長が折角長くなったにもかかわらず、すべてのユーザの使用している鍵長は増加していない。この場合、暗号アタ

ックするほうでは、アタックする鍵長の範囲をもとの鍵長に限定して攻撃することも可能である。これでは、暗号アルゴリズムの許容する鍵長を折角長くとっても実質的に暗号強度を増加させたことにならない。

【０４２６】

このような事態を回避するためには、前述の図１５に示したような鍵長を長くとる方法が有効と考えられる。

【０４２７】

この場合、すべてのユーザは任意に乱数に基づいて鍵長を付加しても、同じものが存在しないため、鍵の管理が容易になるものと考えられる。

【０４２８】

新しく、システムに参加するユーザに対してのみ同一の鍵が存在しないように配慮すれば良い。

【０４２９】

ここで示した、新しい暗号アルゴリズムに対して、ユーザが自分の所有する秘密鍵と公開鍵とを自ら生成する方法は、前述の図１３、図１４、図１１で述べた通常の暗号アルゴリズム変換に対しても適用可能である。ユーザが自分の所有する秘密鍵を生成すれば、鍵管理用ワークステーションから解読される可能性を回避することができる。以下、図２０を参照して、暗号アルゴリズム変換に対してユーザが自分の所有する秘密鍵を生成する形態について説明する。

【０４３０】

この場合の暗号アルゴリズム変換においても、スクランブル機能、デスクランブル機能などを確認する必要があるが、これは、図１３、図１４、図１１で述べた方法と全く同じであるため、ここでは暗号アルゴリズムの配信とユーザが自分の所有する秘密鍵を生成する方法に限定して述べることとする。

【０４３１】

ここで述べる公開鍵暗号方式の運用形態は、図１６に示す暗号化通信方式をとるものとし、図２０はこの暗号化通信方式において、暗号アルゴリズム変換の実施形態を示したものである。

【０４３２】

この図において、受信側ユーザの運用している暗号アルゴリズムをＥＢＦとし、変換する暗号アルゴリズムをＥＡＮＧとする。

【０４３３】

図１３、図１４、図１１で述べた時と同じように、鍵管理用ワークステーションが暗号アルゴリズムＥＢＦに対して運用するマスター鍵としての秘密鍵をｄｃとし、この秘密鍵に対応する公開鍵をQ_cとする。

【０４３４】

同様に、暗号アルゴリズムをＥＡＮＧ対して鍵管理用ワークステーションが運用するマスター鍵としての秘密鍵をd_{cg}とし、この秘密鍵に対応する公開鍵をQ_{cg}とする。

【０４３５】

一方、受信側ユーザが暗号アルゴリズムＥＢＦに対して、運用するマスター鍵としての秘密鍵をd_{YID}とし、この秘密鍵に対応する公開鍵をQ_{YID}とする。

【０４３６】

以上の前提条件は、図１３，１４，１１で示したものと同じであり、以下暗号アルゴリズム変換の実施形態について説明する。

【０４３７】

（１）鍵管理用ワークステーションのネットワーク鍵管理機能は，変換前の暗号アルゴリズムＥＢＦを使用して、以下の暗号文及び、署名データを作成する。

【０４３８】

１：　変換前の暗号アルゴリズムＥＢＦで暗号アルゴリズムＥＡＮＧを暗号化するためのスクランブル鍵K_{SB}，復号化するためのデスクランブル鍵K_{DB}を生成する。

【０４３９】

２：　暗号アルゴリズムＥＡＮＧをスクランブル鍵k_{SB}で暗号化し、暗号文EBF_{KSB}（ＥＡＮＧ）を作成する。

【０４４０】

また、受信側ユーザのマスター鍵としての公開鍵Q_{YID}を取りだし、デスクラ

ンブル鍵K_{DB}を暗号化し、暗号文$EBF_{QYID}(K_{DB})$を作成する。

【０４４１】

３：　変換前の暗号アルゴリズムＥＢＦと鍵管理用ワークステーションのマスター鍵である秘密鍵d_cで、暗号アルゴリズムＥＡＮＧに対し署名作成演算を実施し、署名データS_{dc}（ＥＡＮＧ）を作成する。

【０４４２】

４：　変換前の暗号アルゴリズムＥＢＦと鍵管理用ワークステーションのマスター鍵である秘密鍵ｄｃで変換後の暗号アルゴリズムＥＡＮＧに適用する鍵管理用ワークステーションのマスター鍵としての公開鍵Ｑｃｇに対して署名作成演算を実施し、署名データ$S_{dc}(Q_{cg})$を作成する。

【０４４３】

５：　作成した２組の暗号文$EBF_{QYID}(K_{DB})$、EBF_{KSB}（ＥＡＮＧ），と２組の署名データS_{dc}（ＥＡＮＧ），$S_{dc}(Q_{CG})$及び、鍵管理用ワークステーションの公開鍵Q_{cg}を受信側ユーザに送付する。

【０４４４】

（２）受信側ユーザの暗号アルゴリズムの取得

受信側ユーザは、暗号アルゴリズムとしてＥＢＦを運用しており、マスター鍵としての秘密鍵d_{YID}、及び暗号アルゴリズムＥＢＦで運用される鍵管理用ワークステーションの公開鍵Q_Cを所有している。

【０４４５】

鍵管理用ワークステーションより送付された暗号文から

１：　マスター鍵として秘密鍵d_{YID}を用いて、暗号文$EBF_{QYID}(K_{DB})$を復号し、デスクランブル鍵K_{DB}を取得する。次にこのデスクランブル鍵K_{DB}を用いて暗号文EBF_{KSB}（ＥＡＮＧ）を復号し、暗号アルゴリズムＥＡＮＧを取得する。

【０４４６】

暗号アルゴリズムＥＢＦにおいて、鍵管理用ワークステーションの公開鍵Q_Cを用いて、署名データS_{dc}（ＥＡＮＧ）と取得した暗号アルゴリズムＥＡＮＧに対して署名検証演算を実施し、取得した暗号アルゴリズムＥＡＮＧが正当な鍵管

理用ワークステーションから送付されたものであることを確認する。

【０４４７】

２：　暗号アルゴリズムＥＢＦにおいて、鍵管理用ワークステーションの公開鍵Q_Cを用いて、署名データS_{dc}（Q_{cg}）と送付された鍵管理用ワークステーションの変換した暗号アルゴリズムＥＡＮＧ上で運用する公開鍵Q_{cg}に対して署名検証演算を実施し、送付された公開鍵が正当な鍵管理用ワークステーションの公開鍵であることを確認する。

【０４４８】

以上のようにして、受信側ユーザは、暗号アルゴリズムＥＡＮＧ及び、鍵管理用ワークステーションの暗号アルゴリズムＥＡＮＧ上で運用する公開鍵Q_{cg}取得した。これより、取得した暗号アルゴリズムＥＡＮＧを暗号アルゴリズム管理ＤＢに登録するとともに、暗号アルゴリズム管理機能により運用する暗号アルゴリズムをＥＢＦだけでなくＥＡＮＧも運用可能となった。

【０４４９】

（３）受信側ユーザの所有する鍵の変換

１：　鍵管理用ワークステーションより送付された暗号アルゴリズムＥＡＮＧに対して、受信側ユーザは新規に自ら所有するマスター鍵としての秘密鍵d_{YIDC}を新規に生成する。

【０４５０】

秘密鍵を生成するための方法として、次の３つが挙げられる。

【０４５１】

（ａ）　暗号アルゴリズムＥＢＦで運用している秘密鍵d_{YID}を暗号アルゴリズムＥＡＮＧの秘密鍵として使用する。

【０４５２】

（ｂ）　図１５で示したように、暗号アルゴリズムＥＢＦで運用している秘密鍵d_{YID}に乱数を付加して秘密鍵d_{YIDC}を新規に生成する。

【０４５３】

（ｃ）　暗号アルゴリズムＥＡＮＧの情報により、まったく新規に秘密鍵d_{YIDC}を生成する。

【０４５４】

これらのうちのいずれかの方法で、受信側ユーザ自ら所有する秘密鍵d_{YIDC}を生成し、この秘密鍵に対応する公開鍵Q_{YIDC}を生成する。

【０４５５】

ここで、前記（ｃ）の方法は、先に述べたように他のユーザの使用する鍵と一致する可能性もあるので、鍵管理用ワークステーションにより、他のユーザの使用する公開鍵がないことを確認する必要がある。

【０４５６】

変換する暗号アルゴリズムＥＡＮＧが楕円曲線暗号の場合、このアルゴリズムのベースポイントをＰとして、公開鍵Q_{YIDC}は、$P \cdot d_{YIDC}$（・は楕円曲線上の演算）で与えられる。

【０４５７】

２：　受信側ユーザは一旦暗号アルゴリズムをＥＢＦに戻し、この暗号アルゴリズムＥＢＦのもとに公開鍵Q_{YIDC}に対して秘密鍵d_{YID}を用いて署名作成演算を実施し、署名データ$S_{dYID}(Q_{YIDC})$を作成し、生成した公開鍵Q_{YIDC}、署名データ$S_{dYID}(Q_{YIDC})$及び受信側ユーザのユーザＩＤとを、鍵管理用ワークステーションに送付する。

【０４５８】

３：　鍵管理用ワークステーションは、暗号アルゴリズムをＥＢＦに戻し、送付されたユーザＩＤをキーとしてネットワーク鍵管理ＤＢを検索し、当該受信側ユーザの公開鍵Q_{YID}を取り出す。次に、この受信側ユーザの公開鍵Q_{YID}を用いて、送付された公開鍵Q_{YIDC}及び署名データ$S_{dYID}(Q_{YIDC})$に対して署名検証演算を実施し、正当な受信側ユーザから送付された公開鍵Q_{YIDC}であることを確認する。

【０４５９】

鍵管理用ワークステーションは、ネットワーク鍵管理ＤＢを検索し、受信側ユーザの公開鍵Q_{YID}を確認しているため、受信側ユーザの成りすましを防止することができる。

【０４６０】

以上により鍵管理用ワークステーションは、変換した暗号アルゴリズムＥＡＮＧにおいて、受信側ユーザが運用する公開鍵Q_{YIDC}を取得した。以降、鍵管理用ワークステーションは、暗号アルゴリズムＥＡＮＧで運用するマスター鍵としての秘密鍵d_{cg}を用いて、受信側ユーザが運用する公開鍵Q_{YIDC}に署名作成演算を実施し、署名データS_{dcg}（Q_{YIDC}）を作成し受信側ユーザに送付すること、及び、スクランブル機能、デスクランブル機能を確認するなど、一連の暗号アルゴリズム変換に関する手続きが必要となるが、これらは、図１３、図１４、図１１で述べた暗号アルゴリズム変換に関する手続きで実施すればよい。

【０４６１】

以上、新しい暗号アルゴリズムに対して、ユーザが自分の所有する鍵を自ら生成する実施の形態について説明した。

【０４６２】

最後に、

（１）共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへの変換

（２）公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへの変換

について説明する。

【０４６３】

（１）共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへの変換について

図８、９、６に共通鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへの暗号アルゴリズム変換の実施形態について説明した。

【０４６４】

この場合、変換前の暗号アルゴリズムをＥＢＦとし、変換後の暗号アルゴリズムをＥＡＮＧとしている。

【０４６５】

共通鍵暗号アルゴリズムから他の公開鍵暗号アルゴリズムへの暗号アルゴリズム変換を実施する場合、この記号にあわせて変換前の共通鍵暗号アルゴリズムをＥＢＦとし、変換後の公開鍵暗号アルゴリズムをＥＡＮＧとして説明を行う。

【０４６６】

変換後の公開鍵暗号アルゴリズムＥＡＮＧは、図８、９、６に示す実施形態に従って、変換前の共通鍵暗号アルゴリズムＥＢＦで暗号化して、配信することができる。

【０４６７】

公開鍵暗号アルゴリズムへ変換する場合、新規に秘密鍵と公開鍵とを生成し、変換した公開鍵暗号アルゴリズムに対して、スクランブル機能、デスクランブル機能を確認する必要が生じるが、この一連の鍵生成と機能確認は、図１３，１４，１１で示した公開鍵暗号アルゴリズムの変換の実施形態に従って、実施することができる。

【０４６８】

（２）公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへの変換について

共通鍵暗号アルゴリズムは、公開鍵暗号アルゴリズムと比較すると署名作成、署名検証の演算がない点が異なる。

【０４６９】

従って、公開鍵暗号アルゴリズムから他の共通鍵暗号アルゴリズムへ変換する場合、図１３，１４，１１で示した公開鍵暗号アルゴリズムの変換の実施形態において、この署名作成及び署名検証の演算を除いた手順で、暗号アルゴリズムの変換を実施することができる。

【０４７０】

以上で、暗号アルゴリズム変換の実施形態について示した。

【０４７１】

図５に示した暗号アルゴリズム変換の実施形態の概要、図８、９、６に示した共通鍵暗号アルゴリズム変換の実施形態、及び、図１３，１４，１１で示した公開鍵暗号アルゴリズムの変換の実施形態において、暗号アルゴリズム変換が正常に実施できたかどうかは、暗号化通信システムのスクランブル機能、デスクランブル機能を動作させ、それぞれ平文データＭＤとして＜アルゴリズム変換後のデスクランブル機能確認終了＞及び、平文データＭＳとして＜アルゴリズム変換確

認試験終了＞を暗号化して送付し、復号されるかどうかで確認している。

【０４７２】

この暗号アルゴリズム変換確認のそれぞれのプロセスにおいて、所要の平文データＭＤ、または平文データＭＳが復号されなかった場合は、＜暗号アルゴリズム変換動作異常＞の応答メッセージを送信し、当該プロセスを再度、実行するものとする。

【０４７３】

図１７、１８および図１３、１４、１１で示した公開鍵暗号アルゴリズム変換の実施形態における暗号アルゴリズム変換のデータのやり取りのプロセスにおいて、公開鍵暗号アルゴリズムでの署名作成データに対する署名検証演算を実施している。この署名検証演算を実施した結果、署名作成データに異常が発生した場合も、＜暗号アルゴリズム変換動作異常＞の応答メッセージを送信し、当該プロセスを再度実行するものとする。

【０４７４】

再実行後も平文データＭＤまたは平文データＭＳが復号されなかった場合、および、署名検証演算を実施した結果、署名作成データに異常が発生した場合も、その段階で＜暗号アルゴリズム変換異常終了＞の応答メッセージを送信し、暗号アルゴリズム変換プロセスを中断するものとする。

【０４７５】

＜暗号アルゴリズム変換異常終了＞の応答が発生した場合は、暗号化通信システムの構成要素を、ハード、ソフトの面から点検する作業を実施するものとする。

【０４７６】

図１３、１４、１１は、公開鍵暗号アルゴリズム変換の実施形態を示しているが、暗号アルゴリズム変換を実施しない場合、すなわち、暗号アルゴリズムが同じで暗号アルゴリズムを配布しない場合は、鍵管理局からユーザの使用する鍵の更新、削除等、鍵配送の手順を与えている。図１７、１８で示した公開鍵暗号アルゴリズム変換の実施形態では、平文データＭＤおよびＭＳによる暗号アルゴリズム変換確認のプロセスについて記述していないが、いうまでもなく、図１３、

１４、１１に示した実施形態にしたがって平文データＭＤおよびＭＳを当該暗号アルゴリズムの公開鍵で暗号化して送付することで、暗号アルゴリズム変換確認を実施するこができる。

【０４７７】

【発明の効果】

本発明によれば、暗号アルゴリズムの配信を安全に、しかも、それに要する時間と手間を削減した状態で、暗号アルゴリズムを変換することができる。

【０４７８】

また、このような暗号アルゴリズムの変換によって、複数のユーザで運用される暗号アルゴリズムが同一の暗号アルゴリズムを共有したり、共有する暗号アルゴリズムを他の暗号アルゴリズムに変更することが可能となる。

【図面の簡単な説明】

【図１】　ネットワーク通信システムを示す説明図である。

【図２】　ネットワーク通信システムの各部の機能構成を示す機能ブロック図である。

【図３】　鍵管理用ワークステーションからアクセスされるデータベースに格納される情報を示す説明図であって、（ａ）ネットワーク暗号アルゴリズム管理データベースに格納される情報、（ｂ）ネットワーク鍵管理データベースに格納される情報を示す。

【図４】　パーソナルコンピュータからアクセスされるデータベースに格納される情報を示す説明図であって、（ａ）暗号アルゴリズム管理データベースに格納される情報、（ｂ）鍵構成管理データベースに格納される情報を示す。

【図５】　本発明を適用した暗号アルゴリズムの変換の概略を示すデータフロー図である。

【図６】　本発明を適用した、共通鍵暗号における暗号アルゴリズム変換を示すデータフロー図である。

【図７】　本発明を適用した、共通鍵暗号における暗号化通信を示すデータフロー図である。

【図８】　本発明を適用した、共通鍵暗号における暗号アルゴリズム変換の手順の前半部を示すフロー図である。

【図９】　本発明を適用した、共通鍵暗号における暗号アルゴリズム変換の手順の後半部を示すフロー図である。

【図１０】　本発明を適用した、共通鍵暗号における暗号鍵の変更を示す説明図であって、（ａ）鍵長が短くなる場合、（ｂ）鍵長が短くなる場合の鍵の変更形態を示す。

【図１１】　本発明を適用した、公開鍵暗号における暗号化通信を示すデータフロー図である。

【図１２】　本発明を適用した、公開鍵暗号における暗号アルゴリズム変換を示すデータフロー図である。

【図１３】　本発明を適用した、公開鍵暗号における暗号アルゴリズム変換の手順の前半部を示すフロー図である。

【図１４】　本発明を適用した、公開鍵暗号における暗号アルゴリズム変換の手順の後半部を示すフロー図である。

【図１５】　本発明を適用した、公開鍵暗号における暗号鍵の変更を示す説明図である。

【図１６】　本発明を適用した、公開鍵暗号アルゴリズムによる暗号化通信システムを示すデータフロー図である。

【図１７】　本発明を適用した、可搬型の情報処理装置における暗号アルゴリズム変換を示すデータフロー図である。

【図１８】　本発明を適用した、可搬型の情報処理装置における、他の形態の暗号アルゴリズム変換を示すデータフロー図である。

【図１９】　本発明を適用した、暗号鍵および暗号アルゴリズムに関するデータベースを示す説明図である。

【図２０】　本発明を適用した、暗号アルゴリズム変換であって、ユーザによって暗号鍵が生成される場合を示すデータフロー図である。

【図２１】　本発明を適用した、公開鍵暗号アルゴリズムにおける暗号化通信システムを示すブロック図である。

【図２２】　ネットワーク通信システムの他の態様を示す説明図である。

【図２３】　本発明を適用した、鍵回復機能の暗号化における作用を示す説明図である。

【図２４】　本発明を適用した、鍵回復機能の復号化における作用を示す説明図である。

【図２５】　本発明を適用した、公開鍵暗号アルゴリズムによる、ＩＣカードを用いた暗号化通信システムを示すブロック図である。

【符号の説明】

１００…パーソナルコンピュータ、１１０…鍵構成管理機能、１２０…暗号アルゴリズム管理機能、１３０…スクランブル機能、１４０…デスクランブル機能、１５０…暗号化通信管理機能、１８０…鍵構成管理データベース、１８１…ユーザ固有鍵データベース、１９０…暗号アルゴリズムデータベース、２００…パーソナルコンピュータ、２１０…鍵構成管理機能、２２０…暗号アルゴリズム管理機能、２３０…スクランブル機能、２４０…デスクランブル機能、２５０…暗号化通信管理機能、２８０…鍵構成管理データベース、２８１…ユーザ固有鍵データベース、２９０…暗号アルゴリズムデータベース、４００…鍵管理局、５００…鍵管理用ワークステーション、５３０…スクランブル機能、５４０…デスクランブル機能、５５０…暗号化通信管理機能、５６０…ネットワーク暗号アルゴリズム管理機能、５７０…ネットワーク鍵管理機能、５８０…ネットワーク鍵管理データベース、５８１…ユーザ固有鍵データベース、５９０…ネットワーク暗号アルゴリズムデータベース、５９５…暗号アルゴリズム生成機能、７００…ＩＣカード、７１０…鍵構成管理機能、７２０…暗号アルゴリズム管理機能、７３０…スクランブル機能、７４０…デスクランブル機能、７５０…暗号化通信管理機能、７８０…鍵構成管理データベース、７９０…暗号アルゴリズムデータベース。

【書類名】　図面

【図１】

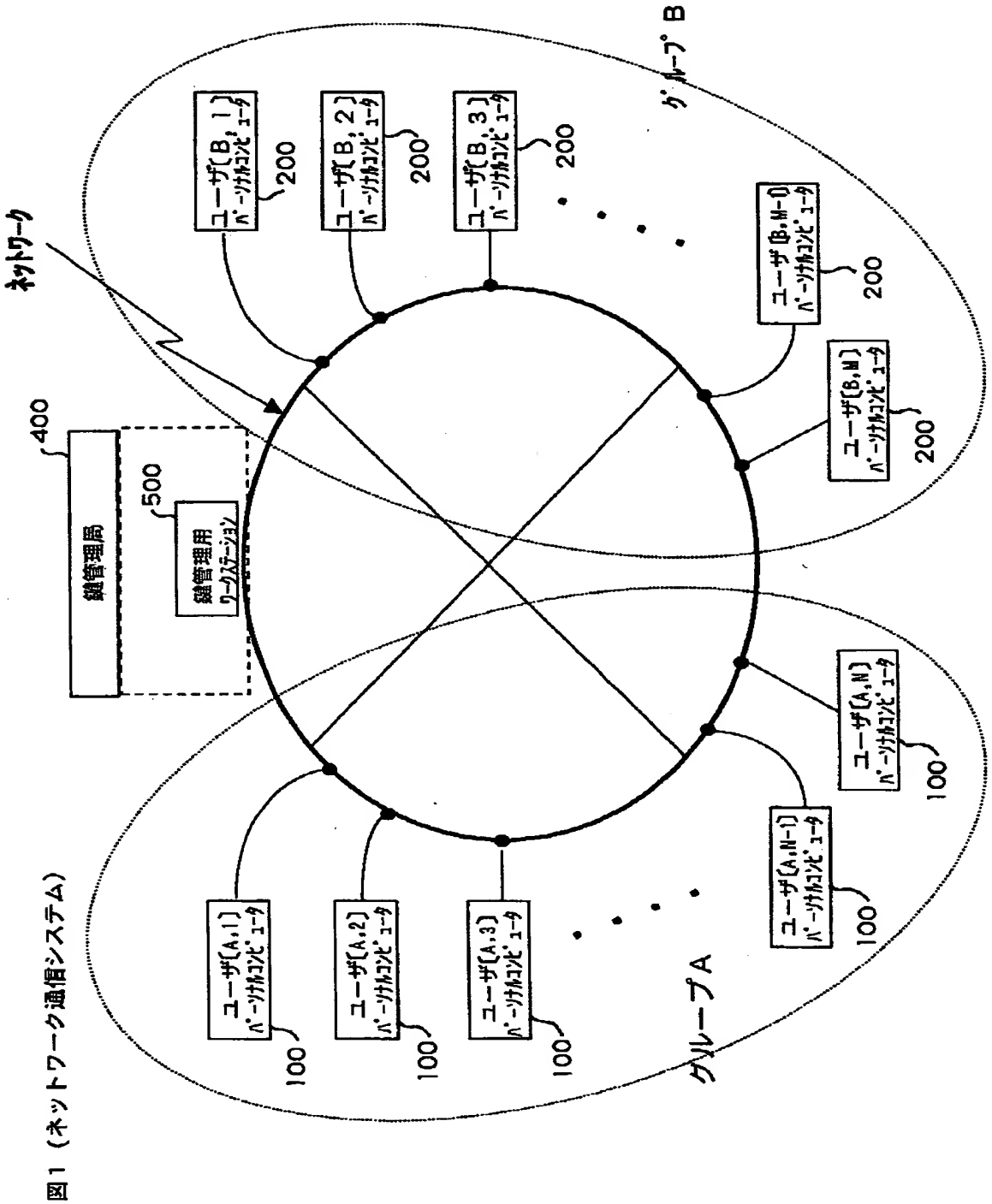


図１（ネットワーク通信システム）

【図２】

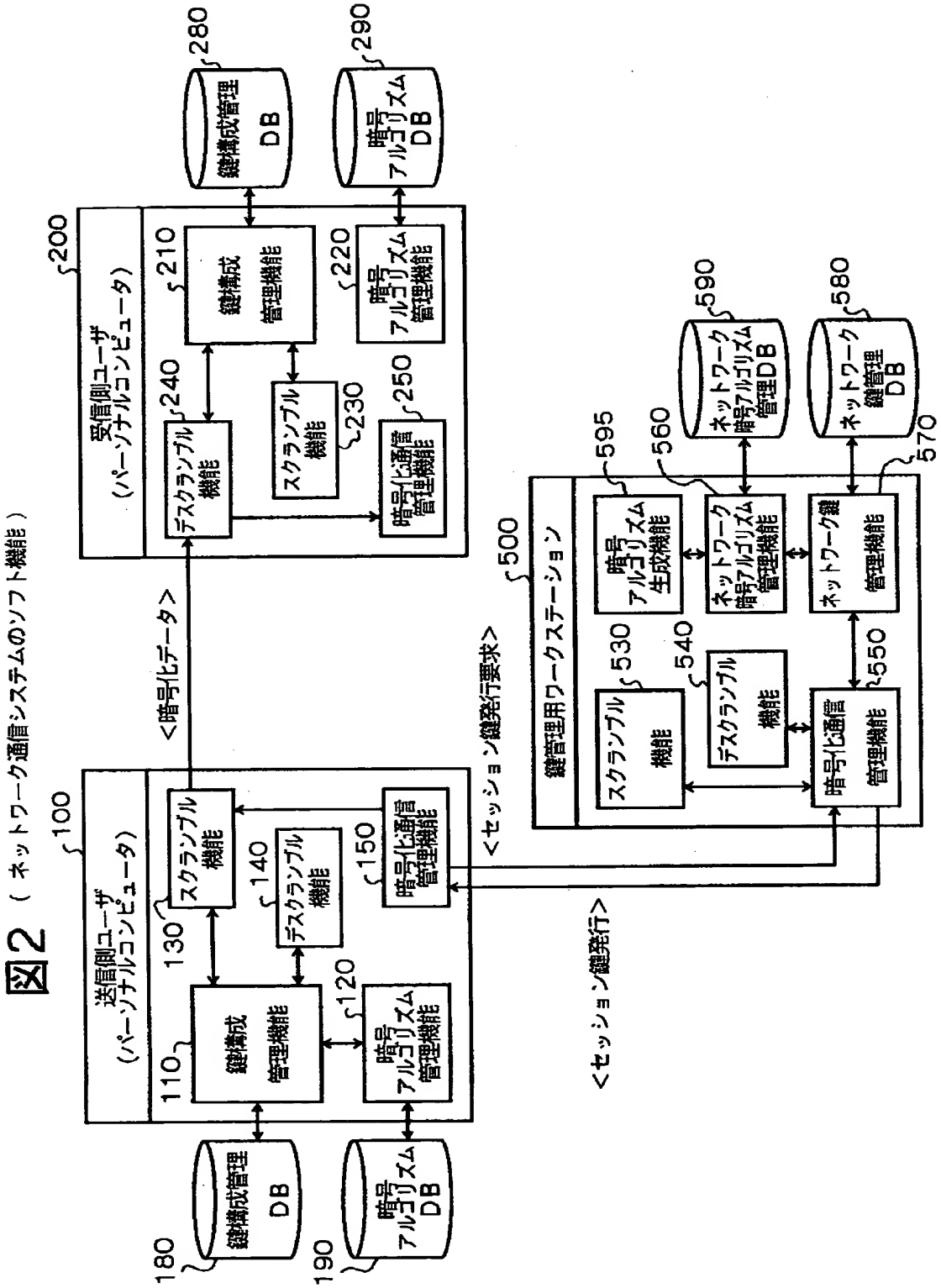


図2（ネットワーク通信システムのソフト機能）
送信側ユーザ（パーソナルコンピュータ）
100
鍵構成管理機能
110
暗号アルゴリズム管理機能
120
スクランブル機能
130
デスクランブル機能
140
暗号化通信管理機能
150
鍵構成管理DB
180
暗号アルゴリズムDB
190
受信側ユーザ（パーソナルコンピュータ）
200
鍵構成管理機能
210
暗号アルゴリズム管理機能
220
スクランブル機能
230
デスクランブル機能
240
暗号化通信管理機能
250
鍵構成管理DB
280
暗号アルゴリズムDB
290
鍵管理用ワークステーション
500
スクランブル機能
530
デスクランブル機能
540
暗号化通信管理機能
550
暗号アルゴリズム生成機能
560
ネットワーク鍵管理機能
570
ネットワーク暗号アルゴリズム管理DB
590
ネットワーク鍵管理DB
580
<暗号化データ>
<セッション鍵発行要求>
<セッション鍵発行>

【図３】

図3

(a) ネットワーク暗号アルゴリズム管理ＤＢ

ユーザＩＤ	暗号アルゴリズム名	暗号アルゴリズムバージョン	更新日時
鍵管理局ＩＤ	暗号アルゴリズム名	暗号アルゴリズムバージョン	更新日時

(b) ネットワーク鍵管理ＤＢ

ユーザＩＤ	暗号アルゴリズム名	暗号アルゴリズムバージョン	鍵情報	更新日時
鍵管理局ＩＤ	暗号アルゴリズム名	暗号アルゴリズムバージョン	鍵情報	更新日時

【図４】

図4

(a) 暗号アルゴリズム管理ＤＢ

暗号アルゴリズム名	暗号アルゴリズムバージョン	更新日時

(b) 鍵構成管理ＤＢ

暗号アルゴリズム名	暗号アルゴリズムバージョン	ユーザ鍵情報	更新日時
暗号アルゴリズム名	暗号アルゴリズムバージョン	鍵管理局の鍵情報	更新日時

【図５】

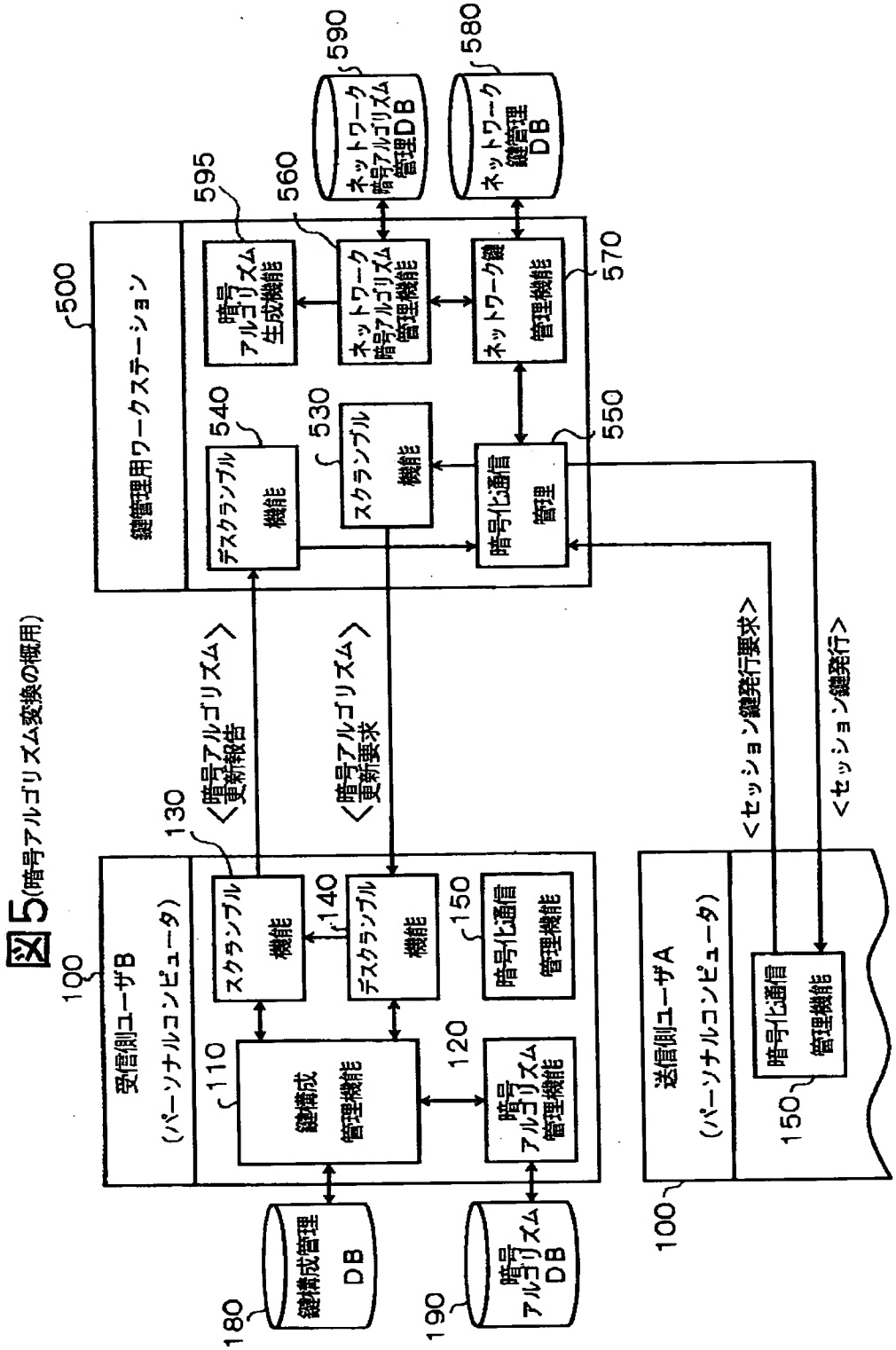


図5（暗号アルゴリズム変換の概用）

【図６】

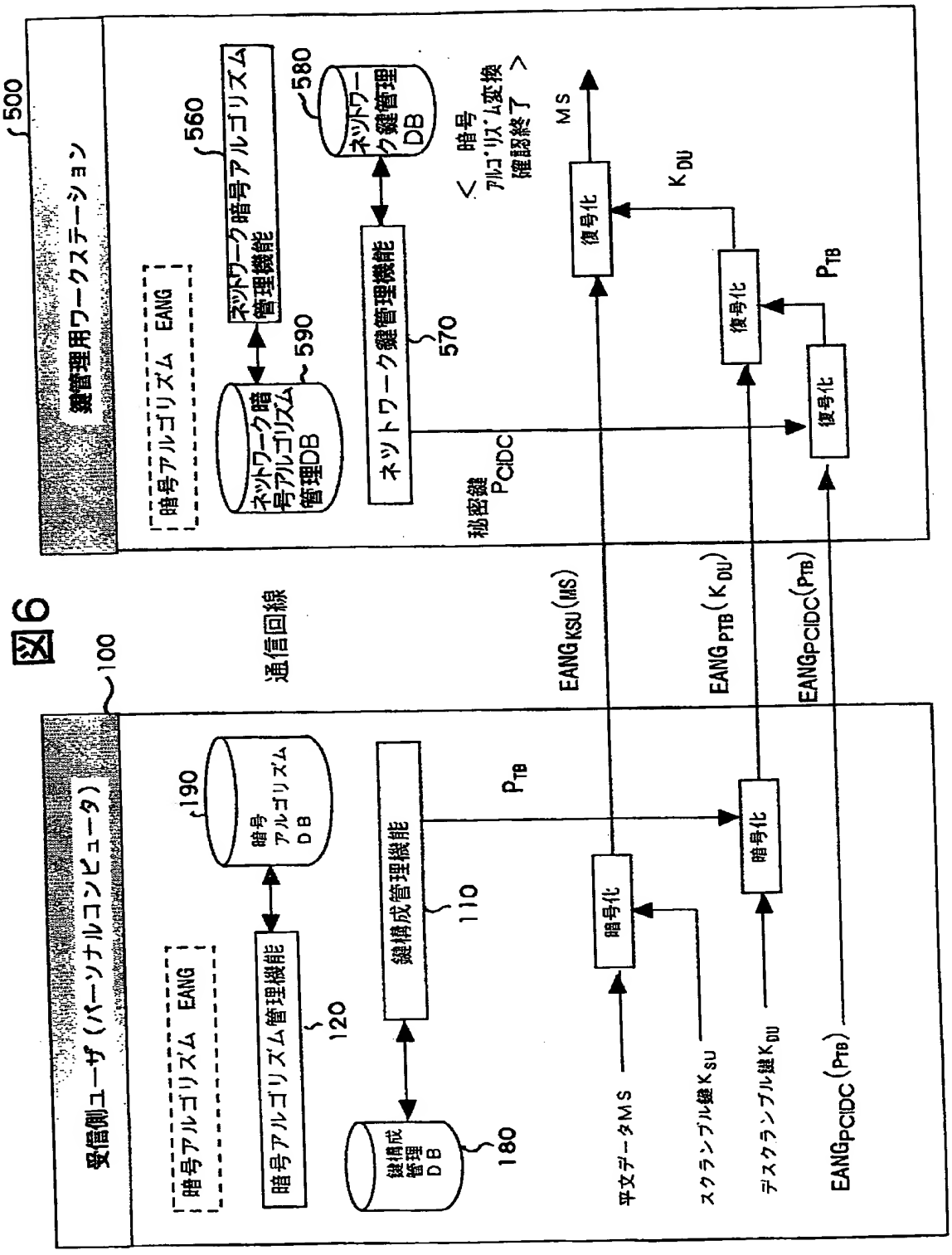


図6
受信側ユーザ（パーソナルコンピュータ）
100
暗号アルゴリズム EANG
暗号アルゴリズム管理機能
120
暗号アルゴリズム DB
190
鍵構成管理DB
180
鍵構成管理機能
110
通信回線
鍵管理用ワークステーション
500
暗号アルゴリズム EANG
ネットワーク暗号アルゴリズム管理機能
560
ネットワーク暗号アルゴリズム管理DB
590
ネットワーク鍵管理機能
570
ネットワーク鍵管理DB
580
秘密鍵 PCIDC
< 暗号アルゴリズム変換確認終了 >
MS
KDU
PTB
暗号化
復号化
復号化
復号化
暗号化
EANGKSU(MS)
EANGPTB(KDU)
EANGPCIDC(PTB)
平文データMS
スクランブル鍵KSU
デスクランブル鍵KDU
EANGPCIDC(PTB)

【図７】

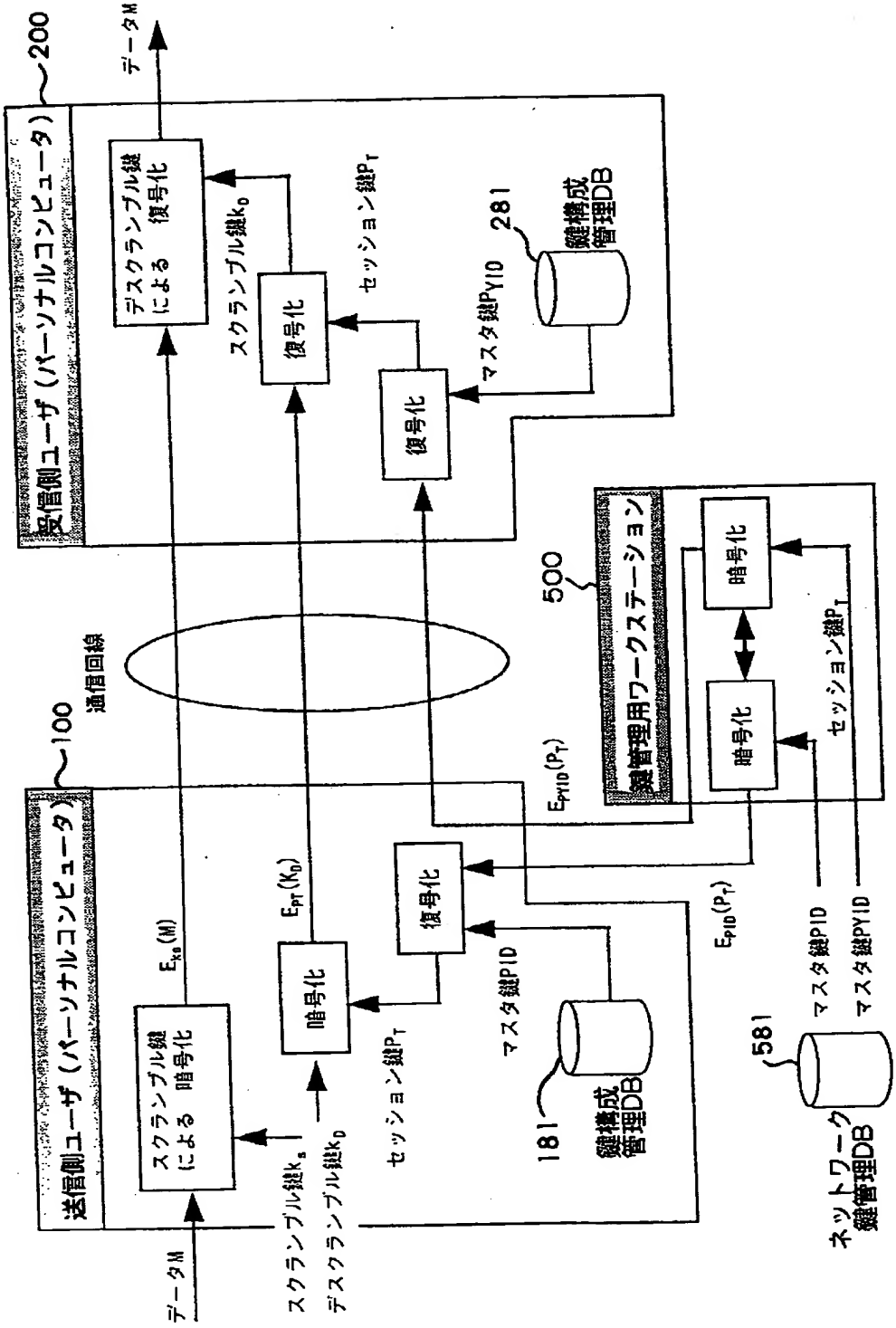
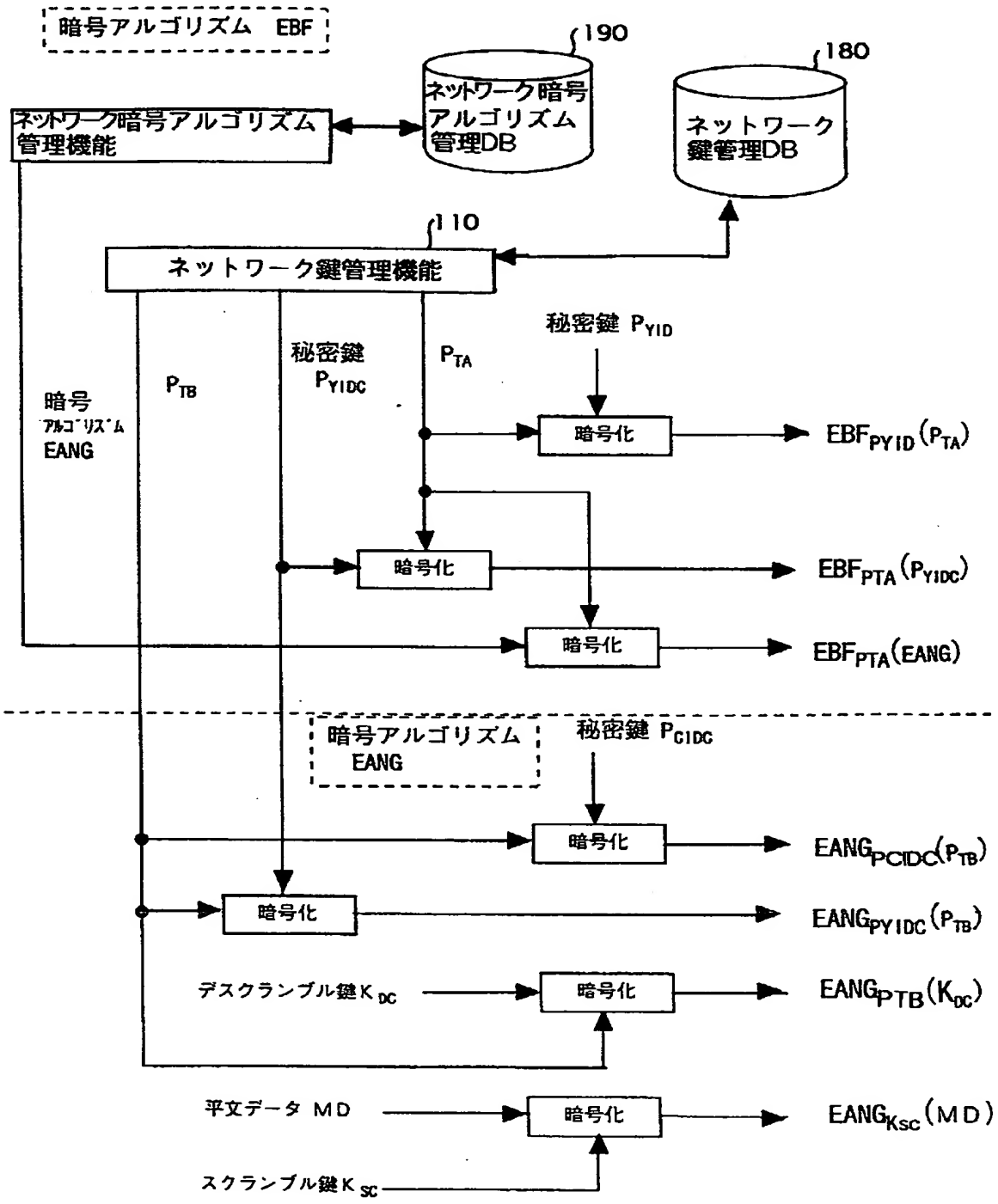


図7 （共通鍵暗号による暗号化通信）

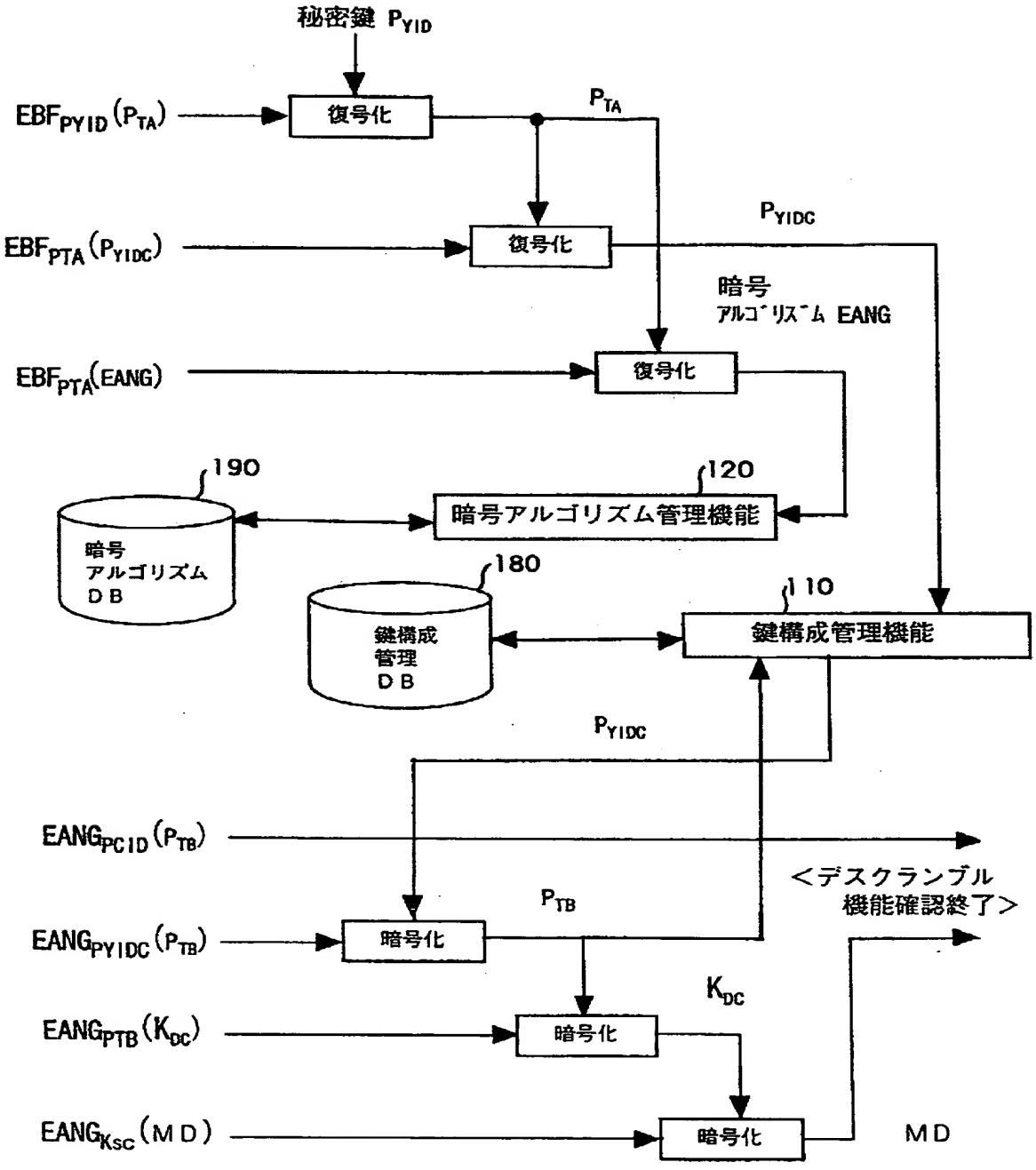
【図８】

図8


暗号アルゴリズム EBF
190
ネットワーク暗号アルゴリズム管理DB
180
ネットワーク鍵管理DB
ネットワーク暗号アルゴリズム管理機能
110
ネットワーク鍵管理機能
秘密鍵 P_{YID}
P_{TA}
秘密鍵 P_{YIDC}
P_{TB}
暗号アルゴリズム EANG
暗号化
$EBF_{PYID}(P_{TA})$
暗号化
$EBF_{PTA}(P_{YIDC})$
暗号化
$EBF_{PTA}(EANG)$
暗号アルゴリズム EANG
秘密鍵 P_{CIDC}
暗号化
$EANG_{PCIDC}(P_{TB})$
暗号化
$EANG_{PYIDC}(P_{TB})$
デスクランブル鍵 K_{DC}
暗号化
$EANG_{PTB}(K_{DC})$
平文データ MD
暗号化
$EANG_{KSC}(MD)$
スクランブル鍵 K_{SC}

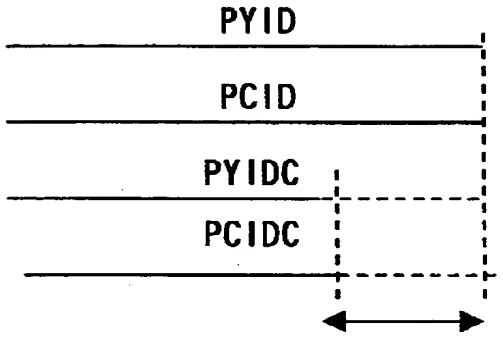
【図９】

図9

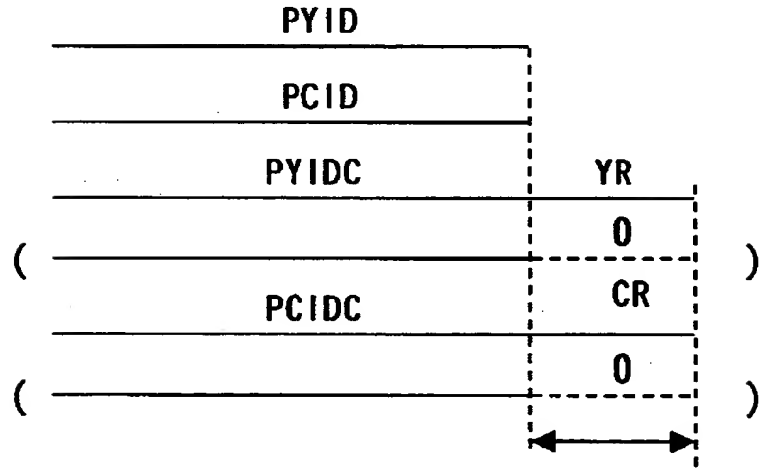

秘密鍵 P_{YID}
$EBF_{PYID}(P_{TA})$
復号化
P_{TA}
$EBF_{PTA}(P_{YIDC})$
復号化
P_{YIDC}
暗号
ｱﾙｺﾞﾘｽﾞﾑ EANG
$EBF_{PTA}(EANG)$
復号化
190
120
暗号
アルゴリズム
ＤＢ
暗号アルゴリズム管理機能
180
110
鍵構成
管理
ＤＢ
鍵構成管理機能
P_{YIDC}
$EANG_{PCID}(P_{TB})$
<デスクランブル
機能確認終了>
P_{TB}
$EANG_{PYIDC}(P_{TB})$
暗号化
K_{DC}
$EANG_{PTB}(K_{DC})$
暗号化
$EANG_{KSC}(MD)$
暗号化
MD

【図１０】

図10



(a)鍵長が短くなる場合



(b)鍵長が長くなる場合

【図１１】

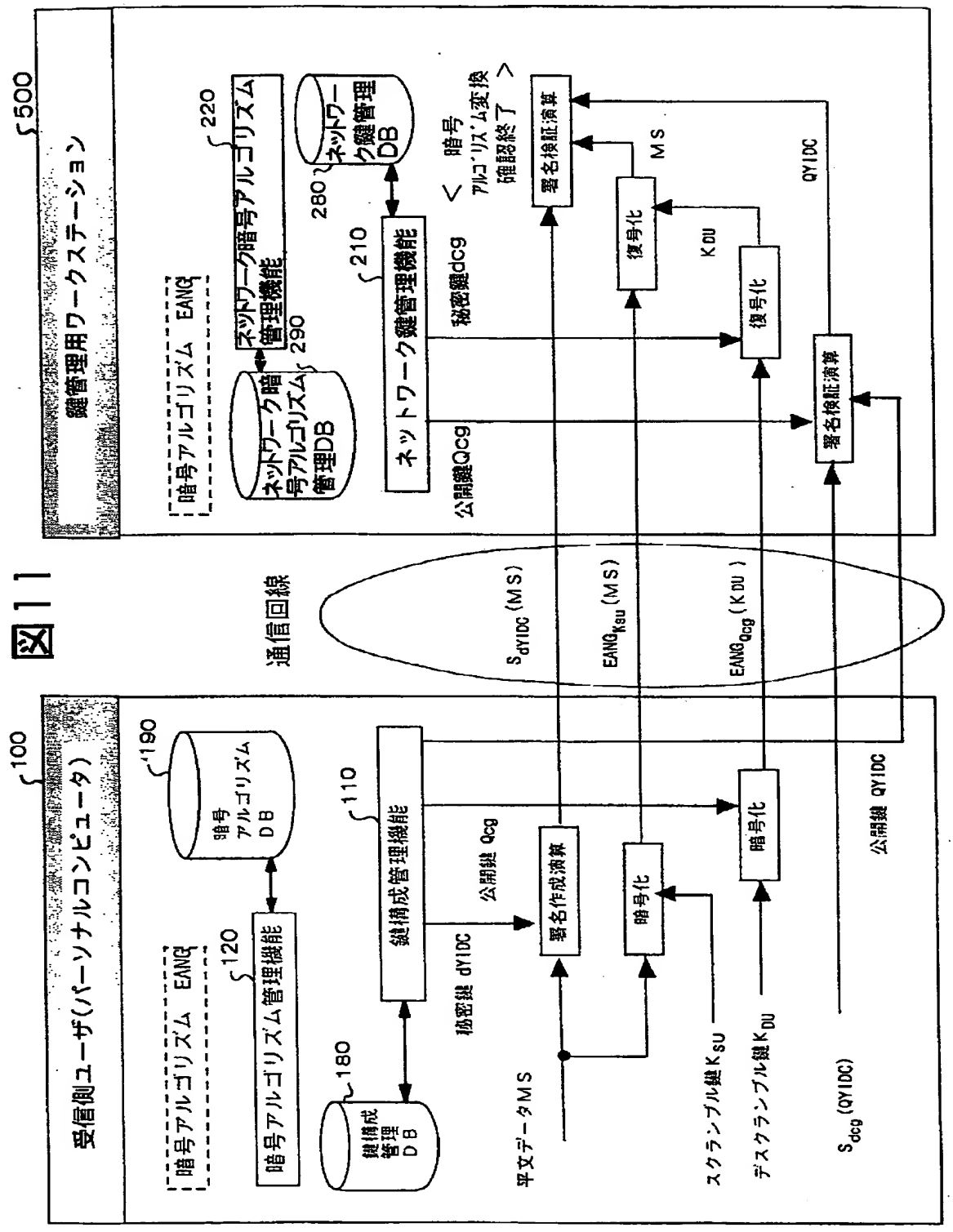

500
鍵管理用ワークステーション
暗号アルゴリズム EANQ
220
ネットワーク暗号アルゴリズム管理機能
290
ネットワーク暗号アルゴリズム管理DB
280
ネットワーク鍵管理DB
210
ネットワーク鍵管理機能
秘密鍵dcg
公開鍵Qcg
< 暗号アルゴリズム変換確認終了 >
署名検証演算
復号化
MS
KDU
復号化
QY1DC
署名検証演算
通信回線
SdY1DC (MS)
EANGKSU (MS)
EANGQcg (KDU)
100
受信側ユーザ(パーソナルコンピュータ)
暗号アルゴリズム EANQ
190
暗号アルゴリズムDB
120
暗号アルゴリズム管理機能
180
鍵構成管理DB
110
鍵構成管理機能
秘密鍵 dY1DC
公開鍵 Qcg
署名作成演算
暗号化
暗号化
公開鍵 QY1DC
平文データMS
スクランブル鍵KSU
デスクランブル鍵KDU
Sdcg (QY1DC)

図11

【図１２】

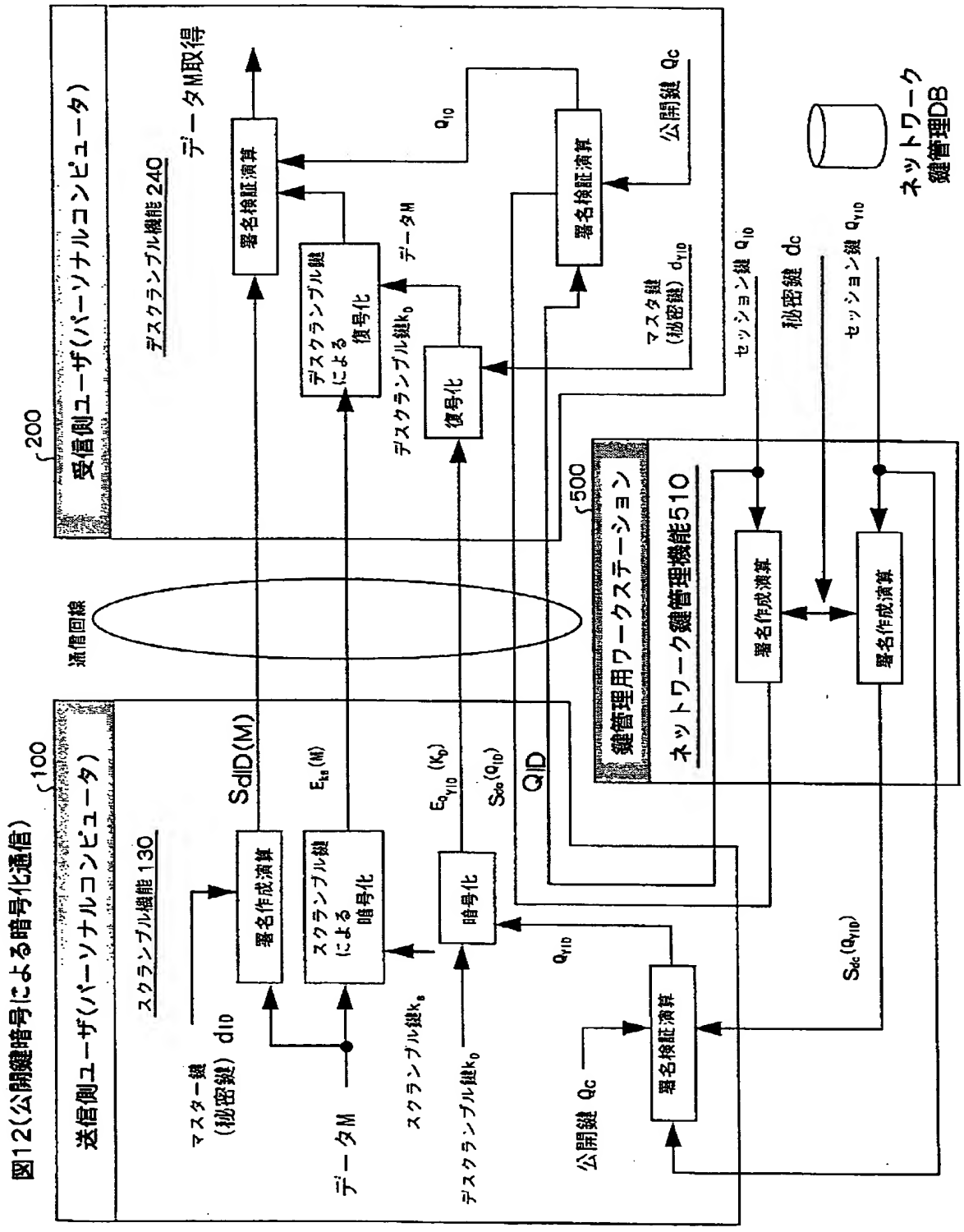
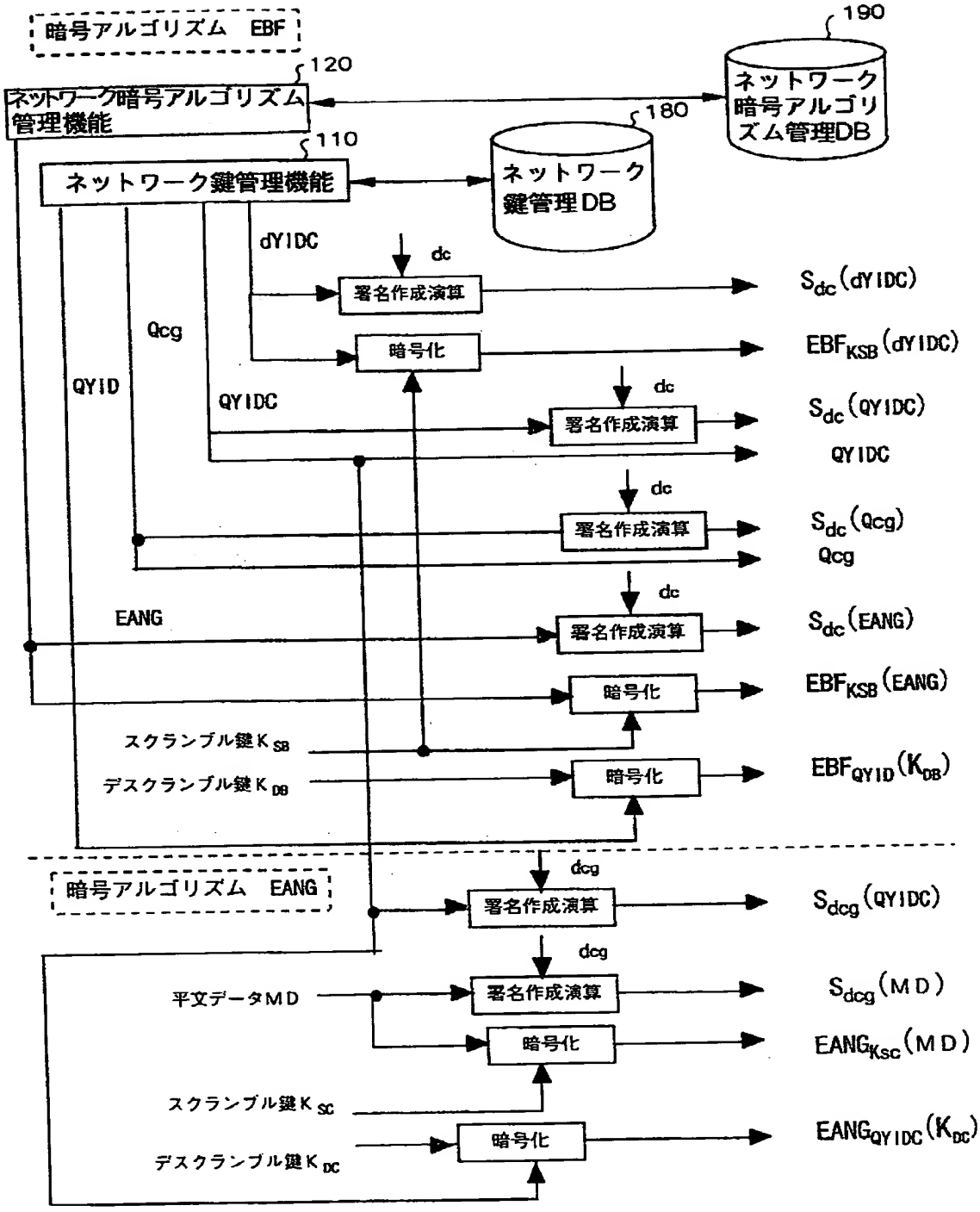


図12(公開鍵暗号による暗号化通信)
100
送信側ユーザ(パーソナルコンピュータ)
スクランブル機能130
マスター鍵
(秘密鍵) dID
データM
スクランブル鍵 k_s
デスクランブル鍵 k_D
署名作成演算
スクランブル鍵による暗号化
暗号化
SdID(M)
$E_{k_s}(M)$
$E_{q_{YID}}(k_D)$
$S_{dc}(q_{ID})$
QID
q_{YID}
公開鍵 q_C
署名検証演算
$S_{dc}(q_{YID})$
通信回線
200
受信側ユーザ(パーソナルコンピュータ)
デスクランブル機能240
データM取得
署名検証演算
デスクランブル鍵による復号化
復号化
デスクランブル鍵 k_D
データM
q_{ID}
署名検証演算
公開鍵 q_C
マスタ鍵
(秘密鍵) d_{YID}
500
鍵管理用ワークステーション
ネットワーク鍵管理機能510
セッション鍵 q_{ID}
秘密鍵 dc
セッション鍵 q_{YID}
署名作成演算
署名作成演算
ネットワーク
鍵管理DB

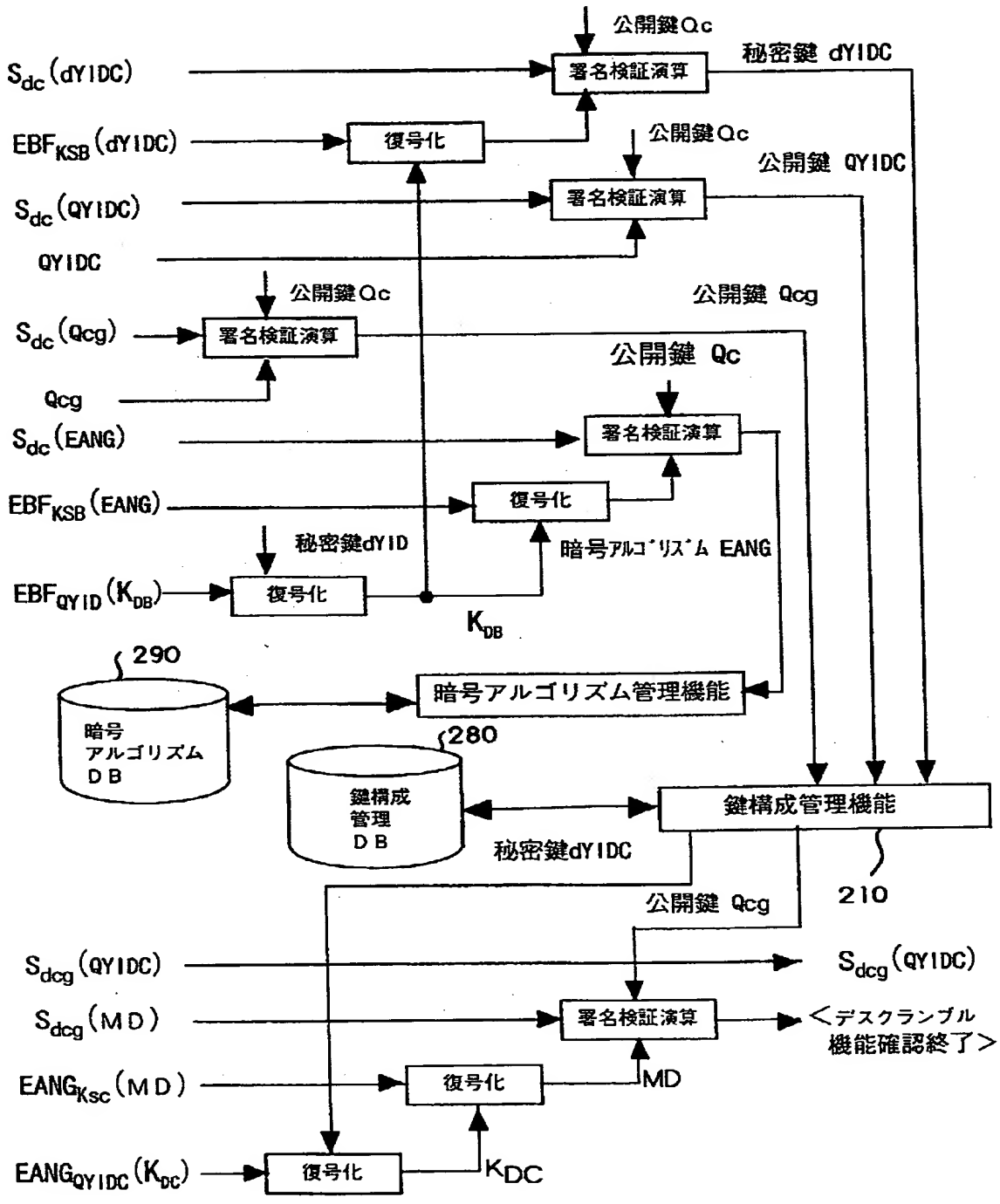
【図１３】

図13


暗号アルゴリズム EBF
120
ネットワーク暗号アルゴリズム管理機能
190
ネットワーク暗号アルゴリズム管理DB
180
ネットワーク鍵管理DB
110
ネットワーク鍵管理機能
dYIDC
dc
署名作成演算
S_{dc}(dYIDC)
暗号化
EBF_{KSB}(dYIDC)
Qcg
QYID
QYIDC
S_{dc}(QYIDC)
QYIDC
S_{dc}(Qcg)
Qcg
EANG
S_{dc}(EANG)
EBF_{KSB}(EANG)
スクランブル鍵 K_{SB}
デスクランブル鍵 K_{DB}
EBF_{QYID}(K_{DB})
暗号アルゴリズム EANG
dcg
S_{dcg}(QYIDC)
平文データMD
S_{dcg}(MD)
$EANG_{Ksc}$(MD)
スクランブル鍵 K_{SC}
デスクランブル鍵 K_{DC}
$EANG_{QYIDC}$(K_{DC})

【図１４】

図14


公開鍵Qc
秘密鍵 dYIDC
S_{dc}(dYIDC)
署名検証演算
EBF_{KSB}(dYIDC)
復号化
公開鍵Qc
公開鍵 QYIDC
S_{dc}(QYIDC)
署名検証演算
QYIDC
公開鍵Qc
公開鍵 Qcg
S_{dc}(Qcg)
署名検証演算
公開鍵 Qc
Qcg
S_{dc}(EANG)
署名検証演算
EBF_{KSB}(EANG)
復号化
秘密鍵dYID
暗号ｱﾙｺﾞﾘｽﾞﾑ EANG
EBF_{QYID}(K_{DB})
復号化
K_{DB}
290
暗号
アルゴリズム
ＤＢ
暗号アルゴリズム管理機能
280
鍵構成
管理
ＤＢ
鍵構成管理機能
秘密鍵dYIDC
210
公開鍵 Qcg
S_{dcg}(QYIDC)
S_{dcg}(QYIDC)
S_{dcg}(ＭＤ)
署名検証演算
<デスクランブル
機能確認終了>
$EANG_{Ksc}$(ＭＤ)
復号化
MD
$EANG_{QYIDC}$(K_{DC})
復号化
K_{DC}

【図１５】

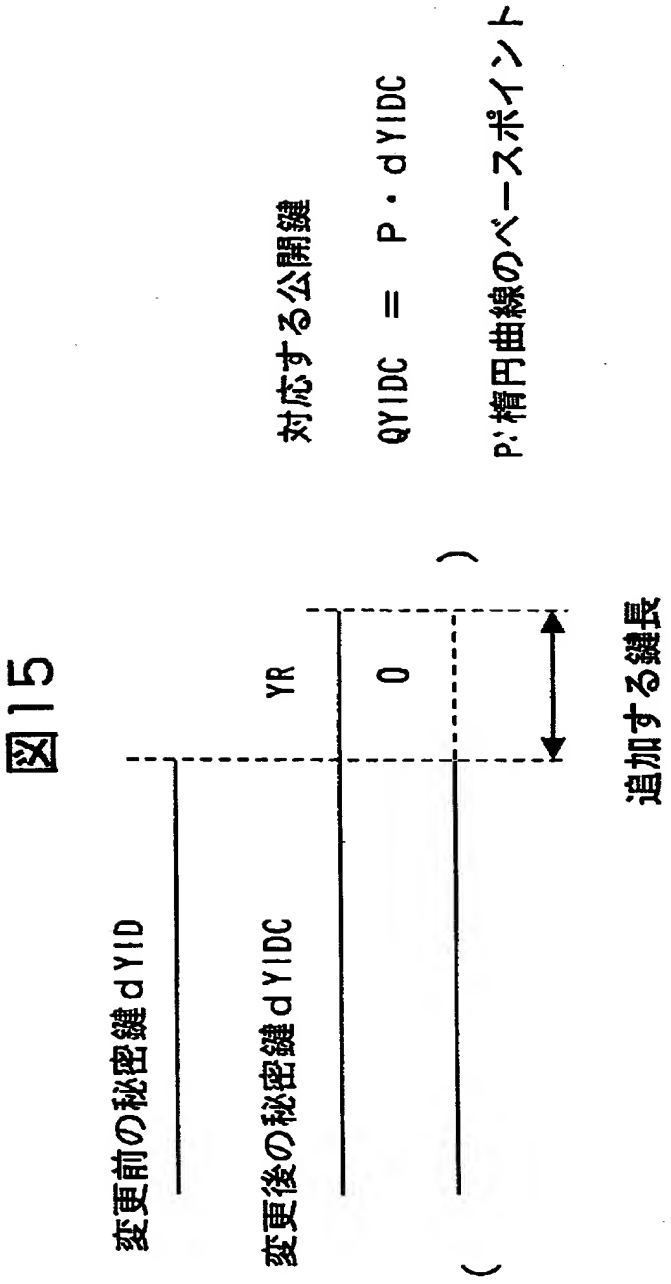


図15
変更前の秘密鍵ｄＹＩＤ
変更後の秘密鍵ｄＹＩＤＣ
ＹＲ
０
（
）
追加する鍵長
対応する公開鍵
ＱＹＩＤＣ　＝　Ｐ・ｄＹＩＤＣ
Ｐ：楕円曲線のベースポイント

【図１６】

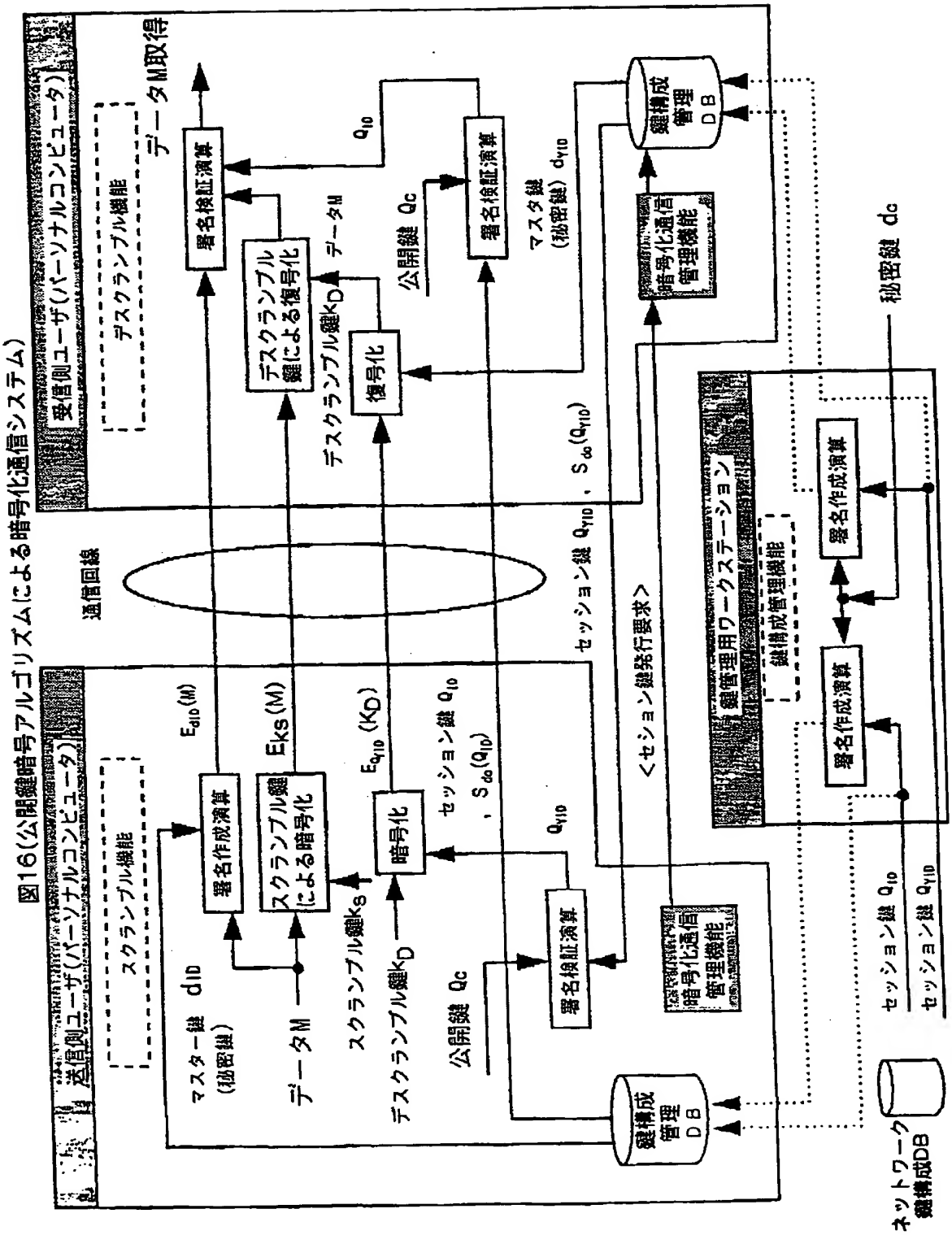


図16(公開鍵暗号アルゴリズムによる暗号化通信システム)
送信側ユーザ(パーソナルコンピュータ)
スクランブル機能
受信側ユーザ(パーソナルコンピュータ)
デスクランブル機能
データM取得
通信回線
マスター鍵 dID (秘密鍵)
データM
スクランブル鍵 kS
公開鍵 QC
署名作成演算
スクランブル鍵による暗号化
暗号化
セッション鍵 QID , Sdo(QID)
署名検証演算
暗号化通信管理機能
鍵構成管理DB
EdID(M)
EkS(M)
EQID(KD)
QYID
<セッション鍵発行要求>
セッション鍵 QYID , Sdo(QYID)
鍵管理用ワークステーション
鍵構成管理機能
署名作成演算
署名検証演算
暗号化通信管理機能
鍵構成管理DB
QID
デスクランブル鍵KD
復号化
デスクランブル鍵による復号化
データM
署名検証演算
公開鍵 QC
マスタ鍵 (秘密鍵) dYID
秘密鍵 dC
セッション鍵 QID
セッション鍵 QYID
ネットワーク鍵構成DB

【図１７】

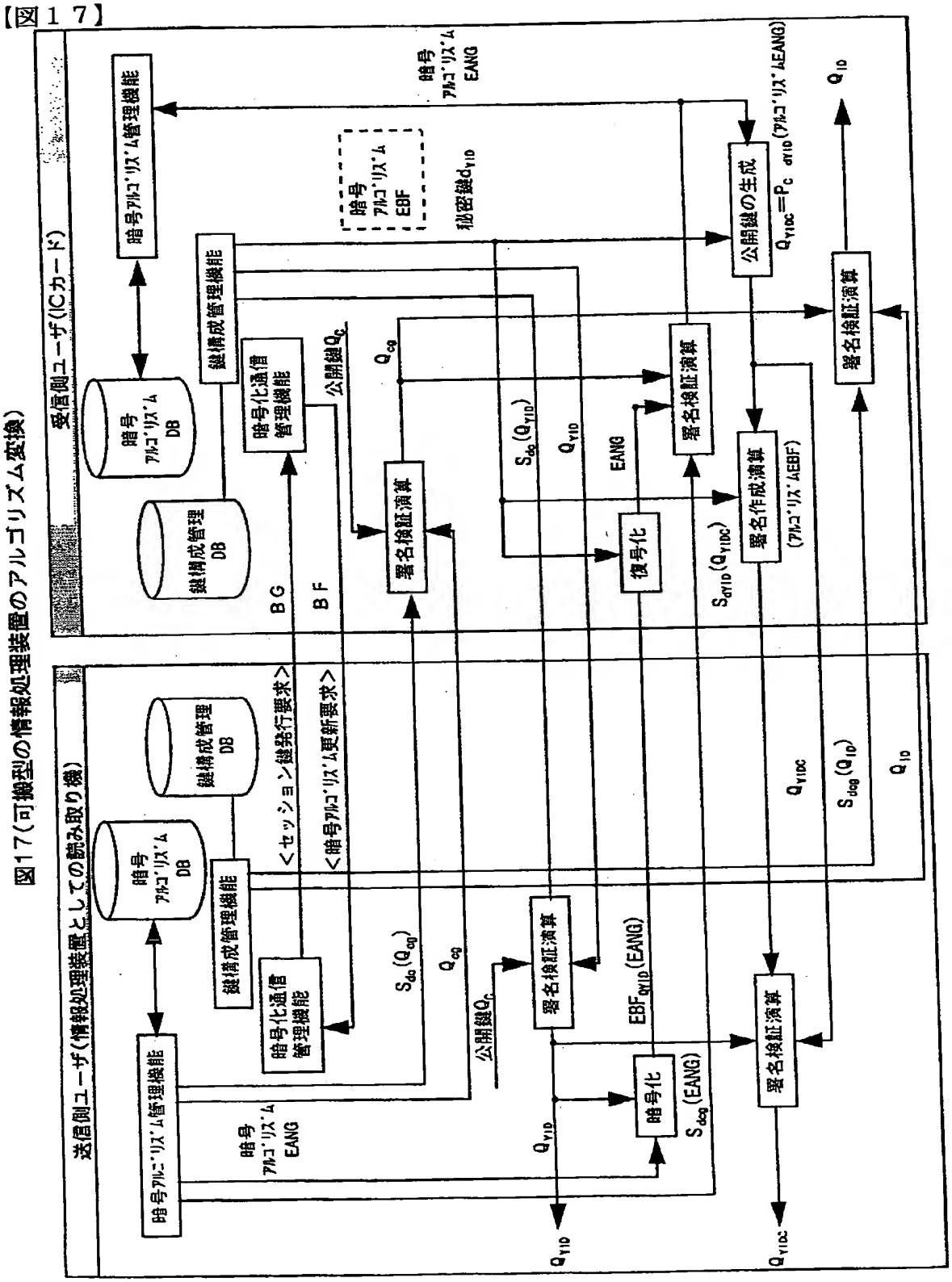


図17(可搬型の情報処理装置のアルゴリズム変換)

【図１８】

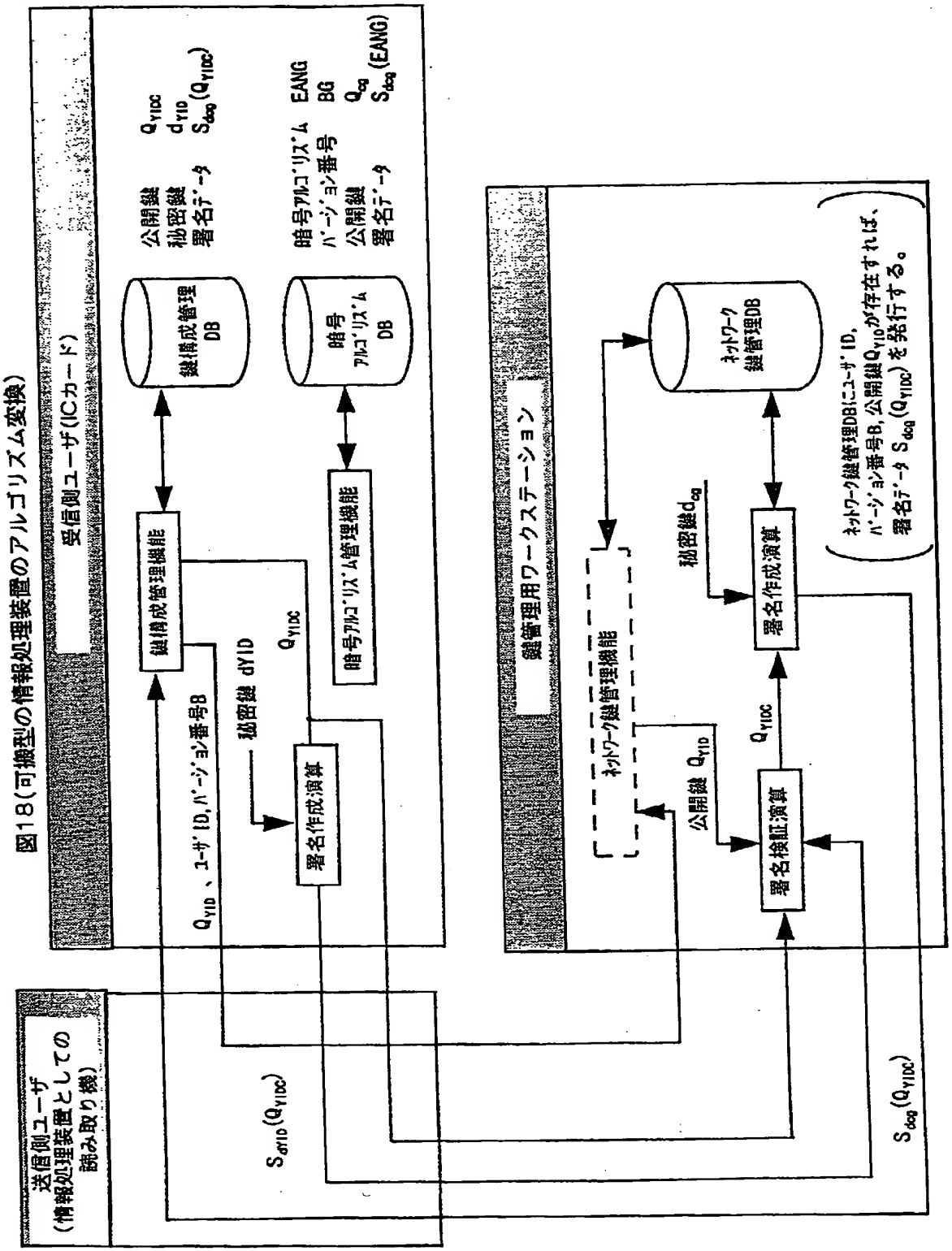


図18(可搬型の情報処理装置のアルゴリズム変換)

【図１９】

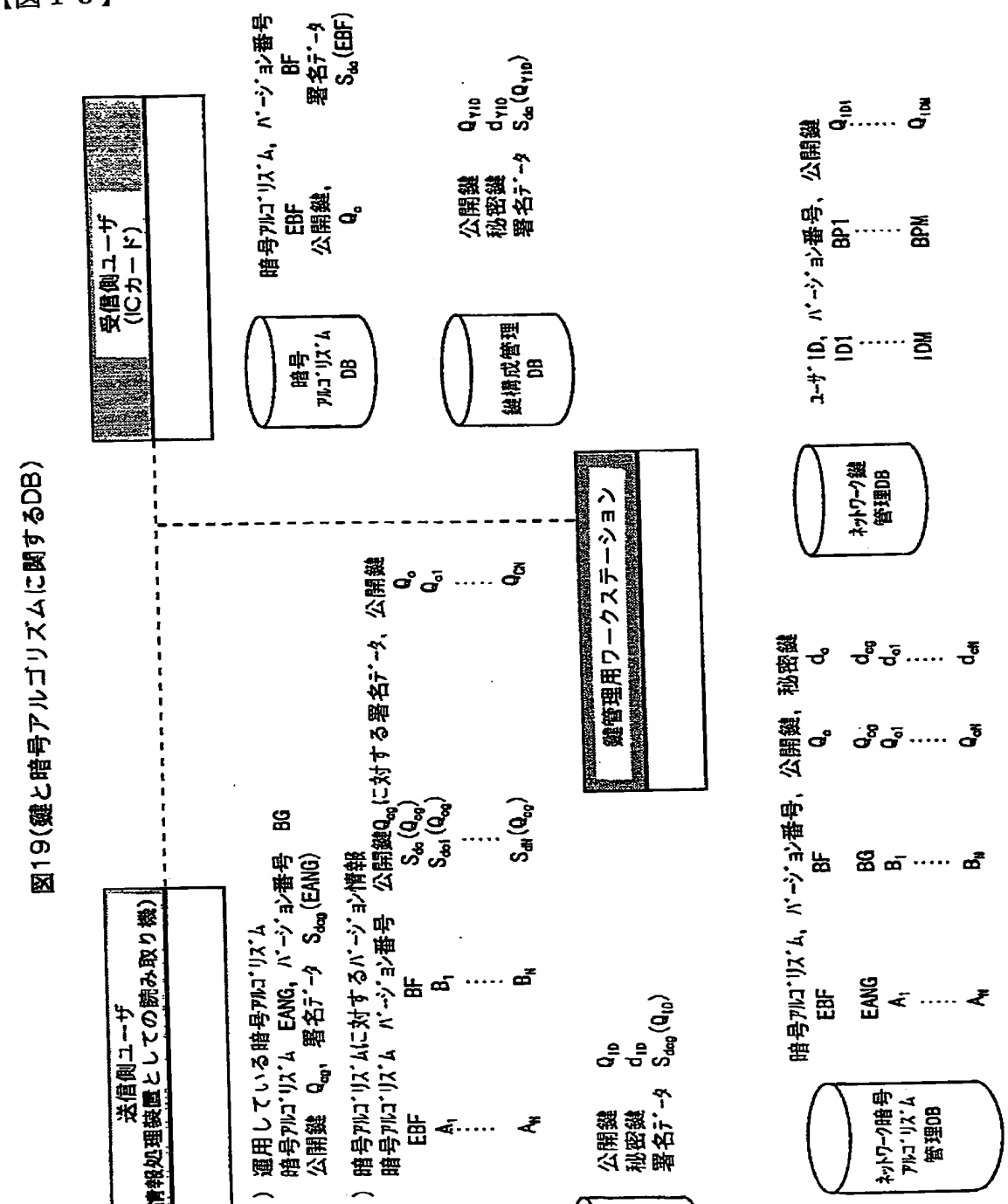


図19(鍵と暗号アルゴリズムに関するDB)
送信側ユーザ
(情報処理装置としての読み取り機)
受信側ユーザ
(ICカード)
暗号アルゴリズムDB
鍵構成管理DB
鍵管理用ワークステーション
ネットワーク鍵管理DB
ネットワーク暗号アルゴリズム管理DB
(1) 運用している暗号アルゴリズム
暗号アルゴリズム EANG, バージョン番号 BG
公開鍵 Q_{eg}, 署名データ S_{deg}(EANG)
(2) 暗号アルゴリズムに対するバージョン情報
暗号アルゴリズム バージョン番号 公開鍵Q_{eg}に対する署名データ, 公開鍵
EBF BF $S_{de}(Q_{eg})$ Q_e
A_1 B_1 $S_{de1}(Q_{eg})$ Q_{e1}
A_N B_N $S_{deN}(Q_{eg})$ Q_{eN}
公開鍵 Q_{ID}
秘密鍵 d_{ID}
署名データ $S_{deg}(Q_{ID})$
暗号アルゴリズム, バージョン番号, 公開鍵, 秘密鍵
EBF BF Q_e d_e
EANG BG Q_{eg} d_{eg}
A_1 B_1 Q_{e1} d_{e1}
A_N B_N Q_{eN} d_{eN}
暗号アルゴリズム, バージョン番号
EBF BF
EANG BG
A_1 B_1
A_N B_N
暗号アルゴリズムDB
公開鍵, 署名データ
EBF Q_{Ye}
公開鍵 Q_{Ye}
秘密鍵 d_{Ye}
署名データ $S_{de}(Q_{Ye})$
ユーザID, バージョン番号, 公開鍵
ID1 BP1 Q_{ID1}
IDM BPM Q_{IDM}

【図２０】

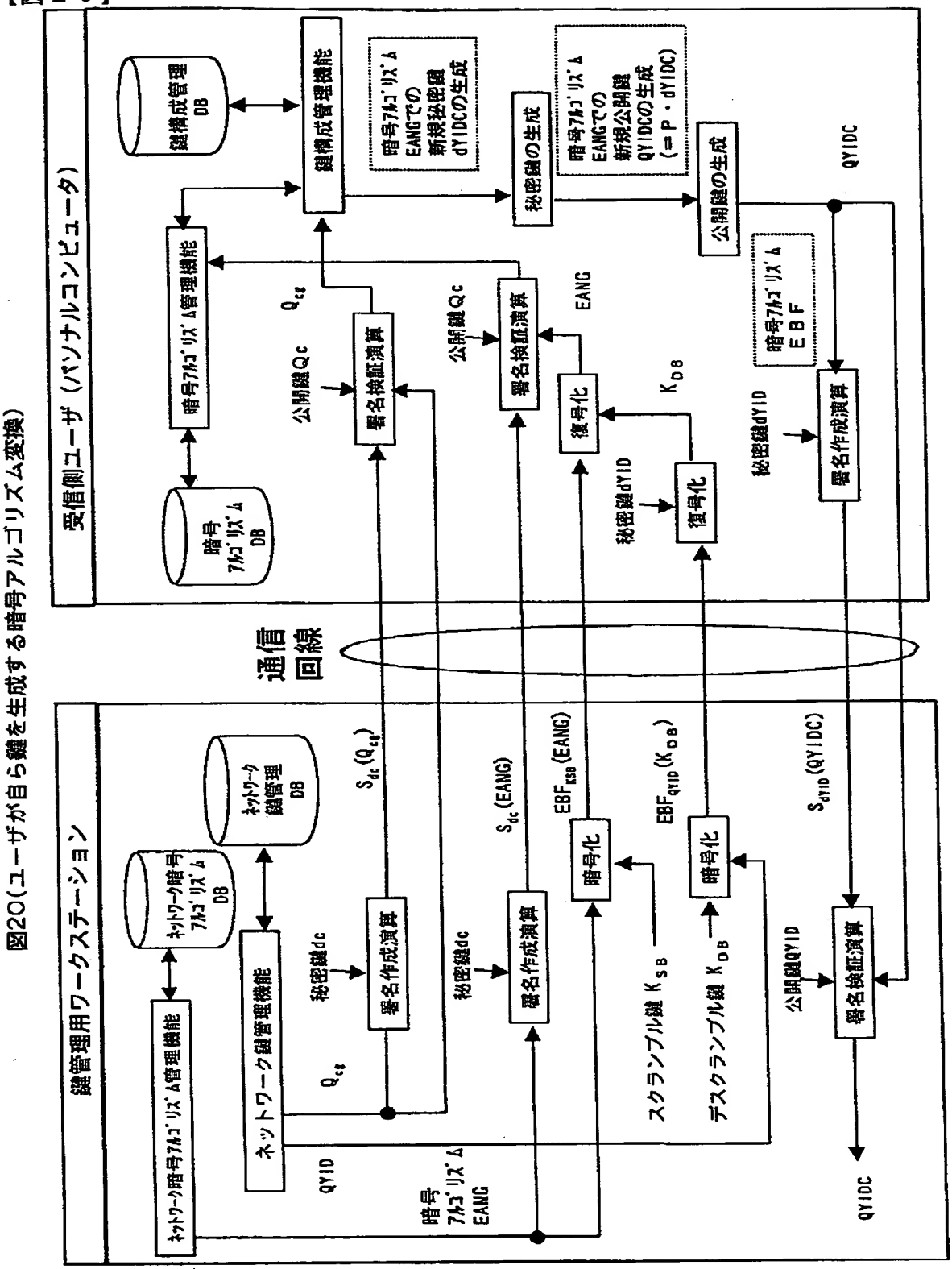
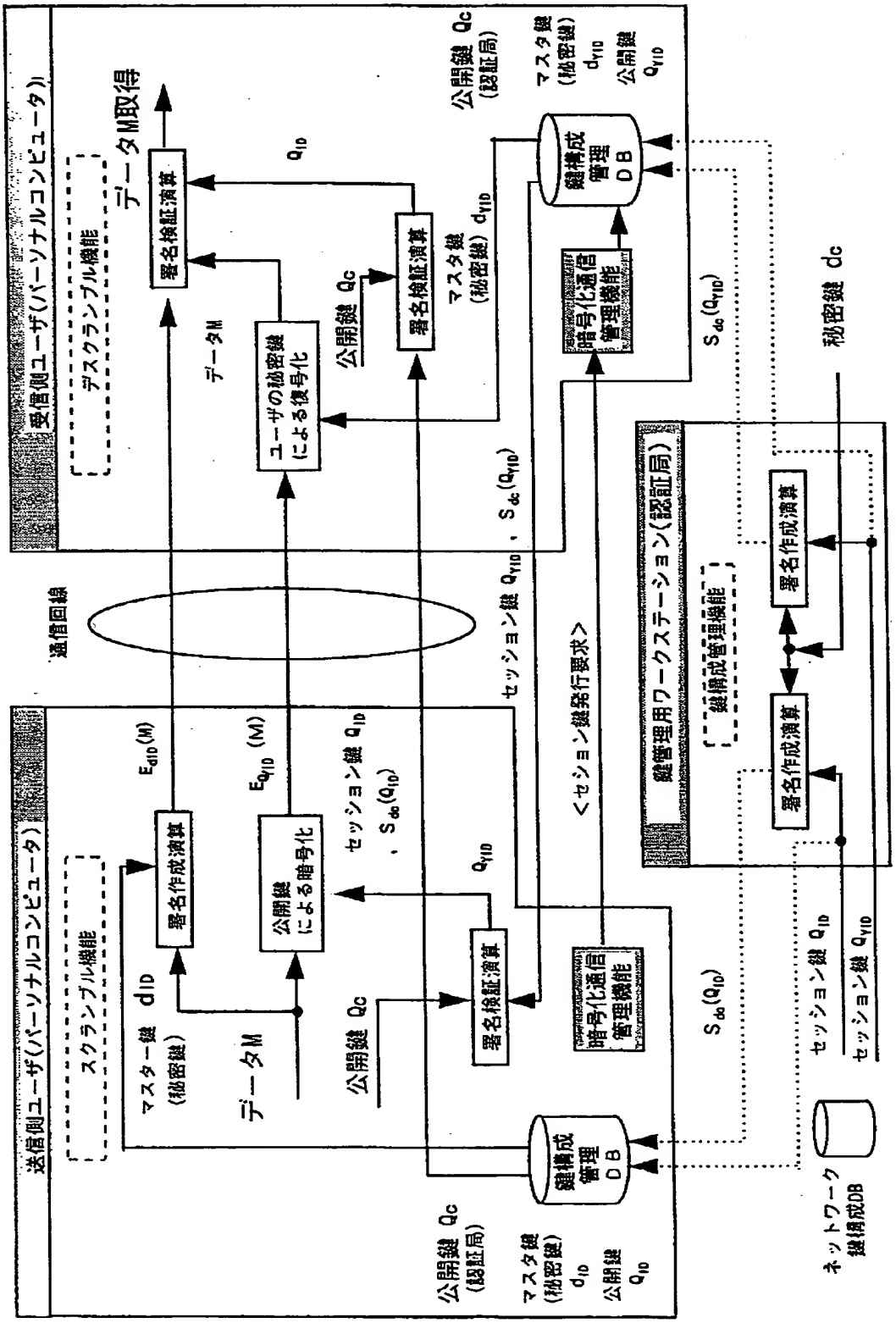


図20(ユーザが自ら鍵を生成する暗号アルゴリズム変換)

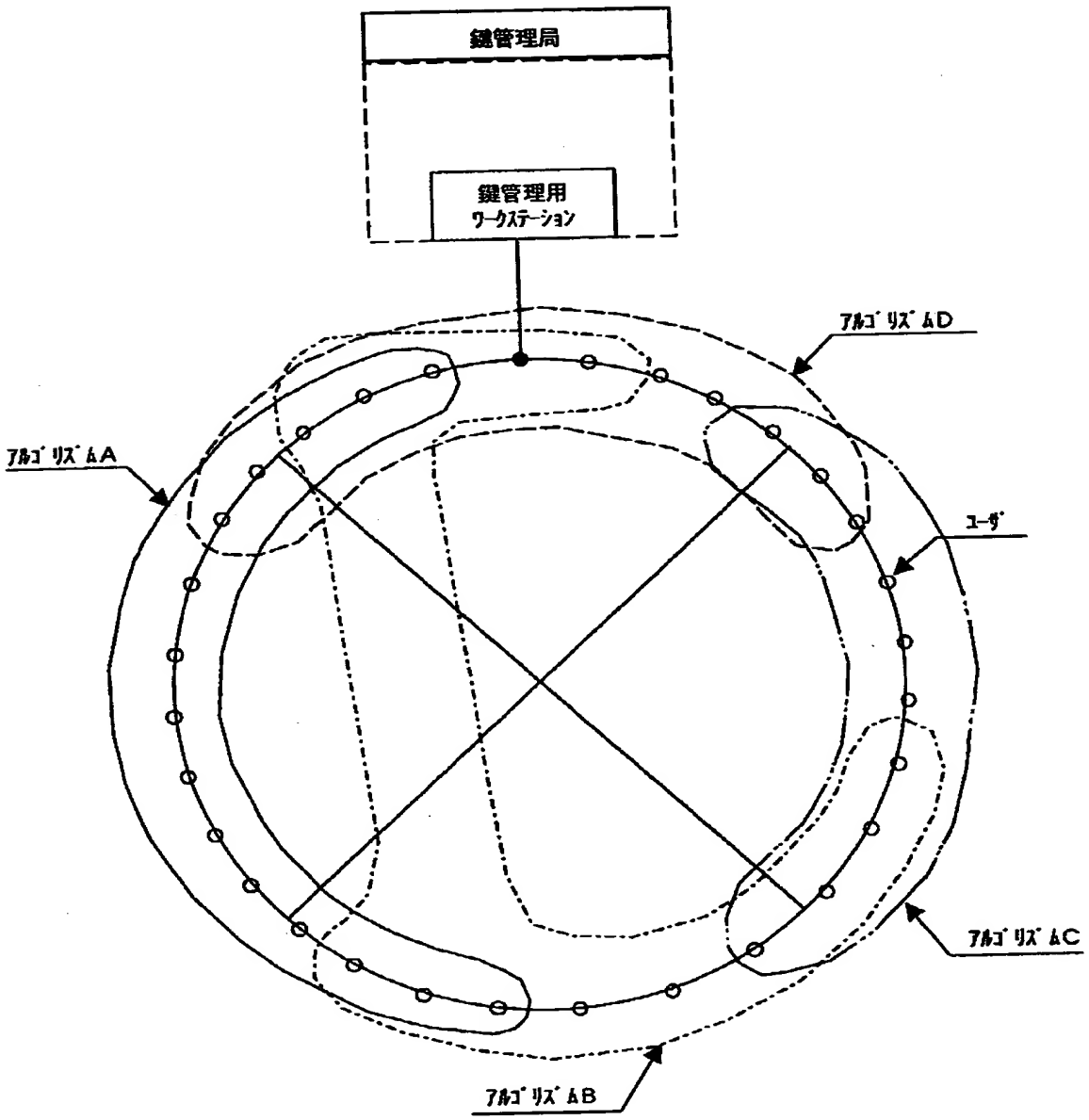
【図２１】

図21（公開鍵暗号アルゴリズムによる暗号化通信システム）



【図２２】

図22(複数の暗号アルゴリズムの存在するネットワーク通信システム)



【図２３】

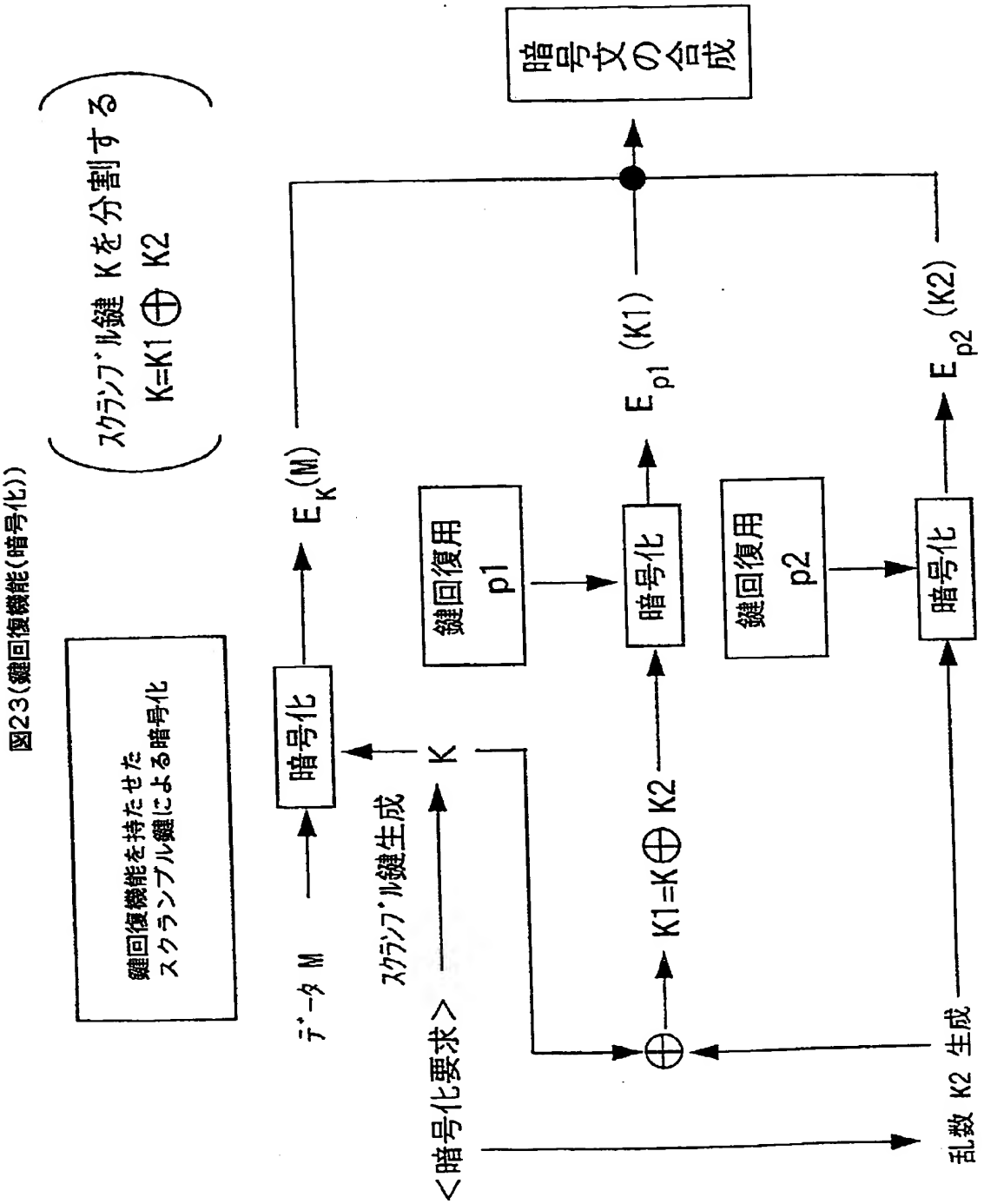


図23(鍵回復機能(暗号化))
鍵回復機能を持たせた
スクランブル鍵による暗号化
データ M
暗号化
$E_K(M)$
スクランブル鍵生成
K
<暗号化要求>
鍵回復用
p1
暗号化
E_{p1} (K1)
K1=K⊕K2
鍵回復用
p2
暗号化
E_{p2} (K2)
乱数 K2 生成
暗号文の合成
スクランブル鍵 Kを分割する
K=K1⊕K2

【図２４】

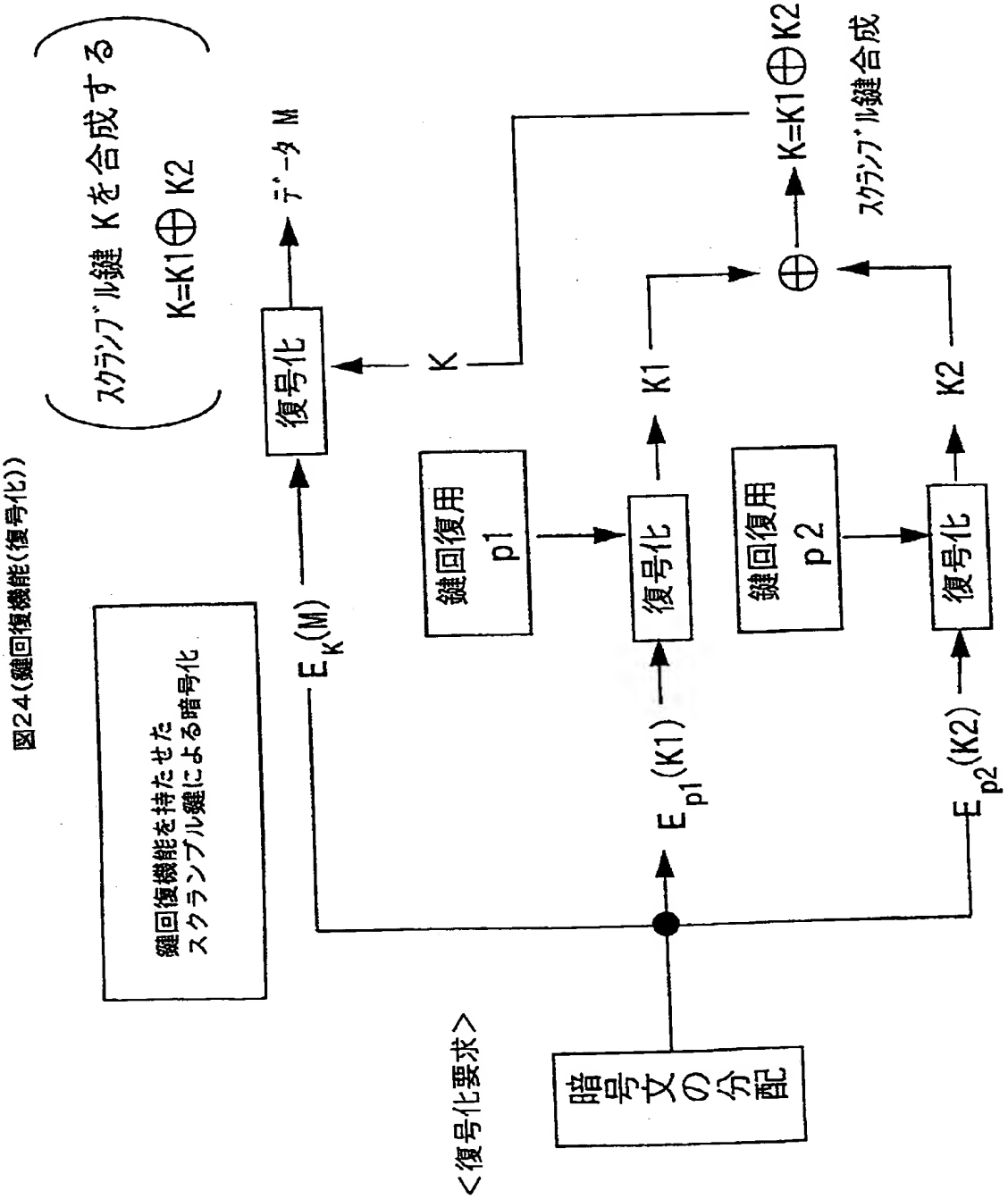


図24（鍵回復機能（復号化））
鍵回復機能を持たせた
スクランブル鍵による暗号化
$E_K(M)$
復号化
K
データ M
（スクランブル鍵 Kを合成する
K=K1⊕K2）
鍵回復用
p1
復号化
K1
鍵回復用
p2
復号化
K2
K=K1⊕K2
スクランブル鍵合成
$E_{p1}(K1)$
$E_{p2}(K2)$
暗号文の分配
<復号化要求>

【図２５】

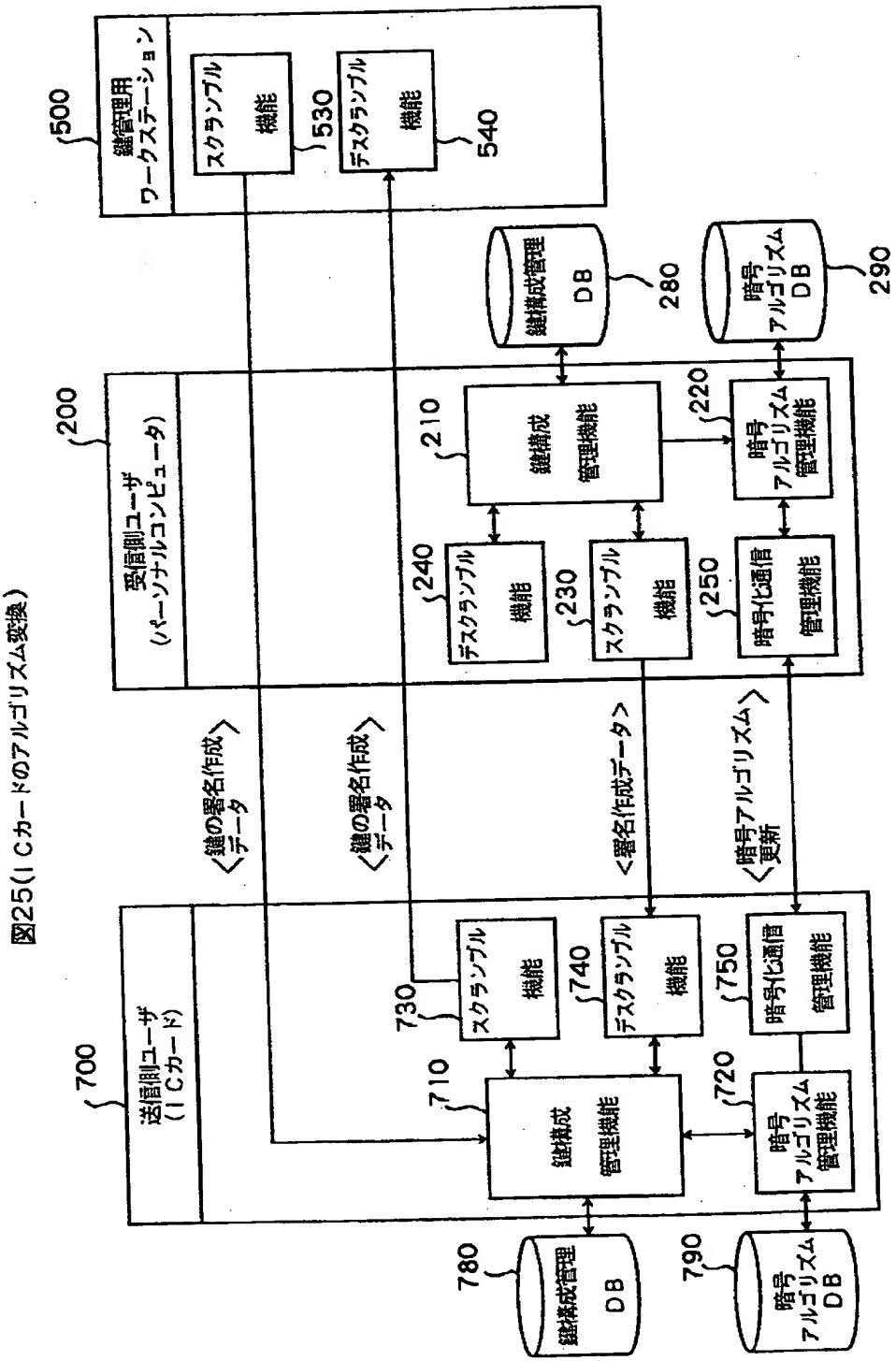


図25(ICカードのアルゴリズム変換)

【書類名】　要約書

【要約】

【課題】　運用する暗号アルゴリズムを別の暗号アルゴリズムに変換する。

【解決手段】　グループＡに属するユーザが使用するパーソナルコンピュータ１００、及び、グループＢに属するユーザが使用するパーソナルコンピュータ２００で相異なる暗号アルゴリズムが運用されるとき、パーソナルコンピュータ１００において、パーソナルコンピュータ２００で運用される暗号アルゴリズムを、パーソナルコンピュータ２００で運用される暗号アルゴリズムで暗号化してパーソナルコンピュータ２００に伝送する。

【選択図】　図１

出証特平１１－３０１８８９１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005108
【住所又は居所】　東京都千代田区神田駿河台四丁目６番地
【氏名又は名称】　株式会社日立製作所
【特許出願人】
【識別番号】　000153421
【住所又は居所】　神奈川県横浜市戸塚区戸塚町２１６番地
【氏名又は名称】　株式会社日立アドバンストシステムズ
【特許出願人】
【識別番号】　000233217
【住所又は居所】　千葉県習志野市東習志野７丁目１番１号
【氏名又は名称】　日立京葉エンジニアリング株式会社
【代理人】　申請人
【識別番号】　100087170
【住所又は居所】　神奈川県横浜市西区北幸２丁目９番１０号　横浜Ｈ
Ｓビル７階
【氏名又は名称】　富田　和子

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出証特平１１－３０１８８９１

出願人履歴情報

識別番号　〔０００１５３４２１〕

１．変更年月日　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市戸塚区戸塚町２１６番地
氏　名　株式会社日立アドバンストシステムズ

出　願　人　履　歴　情　報

識別番号　　〔０００２３３２１７〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　千葉県習志野市東習志野７丁目１番１号
氏　名　日立京葉エンジニアリング株式会社